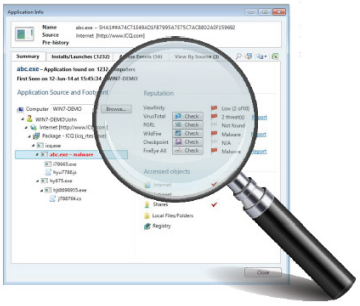
CyberArk 終端特權管理器
CyberArk Endpoint Privilege Manager

在端點上強制實施特權安全防護，同時撤銷本機管理員權限，不會造成不良影響。

挑戰

當攻擊繞過周邊和端點安全而侵入您的環境時，必須有可靠的偵測技術才能迅速回應，並試著防止攻擊範圍擴大。攻擊者會竊取認證、提升特權，並進一步深入您的網路尋找有用的資訊。在端點上強制實施特權安全防護藉此減少攻擊面向，就能為您的安全方案打好基礎。然而，這樣做的缺點就是可能會影響使用者的生產力，連帶增加桌面支援團隊的負擔及相關成本。



集中檢視所有特權原則、應用程式及應用程式信譽。

為有效減少攻擊面向並降低資料遭到嚴重侵害的風險，同時不影響生產力，組織應在端點上實作強制保障特權安全的工具，以封鎖並防堵攻擊。建議的做法是針對企業和系統管理使用者強制實施彈性的最小特權原則，控管允許執行的應用程式，以及確保組織能夠對於經常成為首要目標的認證進行偵測並封鎖攻擊行為。若未能備妥這類工具，組織將面臨下列挑戰：

- **喪失企業生產力。**當組織撤銷企業使用者的所有特權時，使用者可能無法再執行特定工作，或使用日常職務上所需的特定應用程式。沒有靈活的特權原則，就可能使企業停滯不前。
- **技術支援中心成本飆高。**當 IT 原則造成企業使用者無法執行必要的日常工作時，使用者就必須向技術支援中心尋求協助，才能恢復必要的許可權。這種情況可能使 IT 成本大幅增加，並使得支援團隊疲於奔命。
- **因「特權窺探」造成安全風險升高。**即使組織撤銷企業使用者的所有特權，IT 團隊有時仍須針對特定工作重新授予特權。然而，特權重新授予後，鮮少會再次撤銷，如此就會因為管理權限過多形成安全漏洞，致使企業門戶洞開。
- **惡意軟體型攻擊的成功機率大增。**即使組織將 Windows 裝置上的使用者特權降至最低限度，仍可能遭受惡意軟體的攻擊，因為這類攻擊不需要特權就能發動。若未備妥輔助工具來控管應用程式執行許可，並且保護攻擊者的主要攻擊目標，也就是認證，那麼攻擊者就能成功利用惡意軟體型攻擊趁隙入侵組織。

解決方案

CyberArk 終端特權管理器 (CyberArk Endpoint Privilege Manager) 能有效撤銷強制實施最小特權時的障礙，讓組織能夠在端點上封鎖及防堵攻擊，降低資訊遭竊或是遭到加密並劫持進而勒索的風險。特權安全與應用程式控管相互結合之下，就能降低遭到惡意軟體感染的風險。不明應用程式只能以受限模式執行，目的在於防堵威脅，而行為分析能夠封鎖嘗試竊取認證的行為。這些重要的防護技術都是透過單一代理部署，能夠強化現有端點的安全性。

CyberArk 終端特權管理器還能讓安全團隊對 IT 管理員強制實施細膩的最小特權原則，協助組織在 Windows 伺服器上有效劃分權利義務。除了這些特權控管功能之外，解決方案當中還提供了應用程式控管功能加以輔助，其設計在於管理及控管哪些應用程式能夠在端點和伺服器上執行。

為何選擇 CyberArk?

CyberArk 是值得信賴的專家，能夠在營運受影響之前防堵外界攻擊。

有了 CyberArk 終端特權管理器，組織就能夠：

- **依據企業需求自動建立原則。**依據信任的來源建立應用程式控管和特權提升原則，像是 SCCM、軟體散發者、更新者等等。
- **對 Windows 系統管理員強制實施細膩的最小特權原則。**安全團隊可從細部控管每一位 IT 管理員能夠依其角色在 Windows 伺服器上執行的命令和工作。
- **視需要順利提升企業使用者特權。**企業使用者的本機管理員許可權撤銷後，CyberArk 終端特權管理器會依據原則提升受信任的應用程式所需的特權。
- **迅速識別並封鎖惡意應用程式。**依據像是 VirusTotal 和 NSRL 等正式發佈的黑名單資料庫自動比對不明應用程式，以迅速識別已知的惡意軟體並更新全域原則，防止這類應用程式在環境中執行。
- **偵測並封鎖嘗試竊取認證的行為。**竊取認證是所有攻擊當中的主要行為。行為分析能夠協助組織偵測並封鎖嘗試竊取 Windows 認證的行為，還包括常用的網頁瀏覽器中存放的認證。
- **讓不明應用程式以受限模式安全地執行。**若是既非受信任、也非已知為惡意的不明應用程式，只能以「受限模式」執行，藉此防止其存取公司資源、機密資料或網際網路。
- **與威脅偵測工具整合，藉此分析不明應用程式。**CyberArk 終端特權管理器能夠將不明應用程式傳送至 Check Point、FireEye 及 Palo Alto Networks 威脅偵測解決方案進行自動化的檔案分析。
- **找出環境中的所有應用程式。**在每一台受保護的機器上運用代理，就能讓解決方案立即找出環境中某一應用程式的所有實例，以及每一個應用程式的源頭。

優勢

- 在攻擊侵入傳統環境周邊時提供一層額外的重要防護和端點安全控管
- 結合各項獨特的技術為端點提供防護，並封鎖及防堵攻擊，降低可能對企業造成的損害
- 強化現有端點安全措施的防護與偵測能力
- 讓桌面團隊能夠輕鬆實施安全原則，並盡可能減少對企業的影響
- 防止使用者安裝未經批准的應用程式及造成工作站不穩定，導致技術支援中心疲於應付及支援成本大增
- 撤銷本機系統管理員許可權，同時兼顧使用者生產力，並且不致增加技術支援中心的負擔
- 採用自動化的原則建立程序讓部署工作更輕鬆，減輕桌面團隊的負擔
- 協助桌面團隊因應安全/風險管理團隊的需求，同時減少其工作量
- 防堵惡意軟體，阻止其擴散至網路，縮短補救時間並減少投入的精力

全方位的解決方案

CyberArk 終端特權管理器屬於 CyberArk 特權帳號安全解決方案整體的一部分，這套完整的解決方案能夠主動防禦進階攻擊，阻止其入侵管理特權而進入企業核心、竊取機密資料及損壞重要的系統。這套解決方案可協助組織消除不必要的本機系統管理員特權，並強化特權帳號的安全性，藉此減少攻擊面向。解決方案內含的產品可單獨管理，也可相互結合，成為整合一致的全方位特權帳號安全解決方案。

規格

支援的平台：

Windows 桌面：

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

Windows Server：

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

全方位應用程式支援：

- 可執行檔
- MSI、MSU
- 系統管理工作
- 管理主控台內嵌式管理單元
- 指令碼
- 登錄設定
- ActiveX 控制項
- COM 物件
- Web 應用程式

兼具彈性與安全性的應用程式規則：

- 檔案路徑比對
- 命令列比對
- 檔案雜湊 (SHA-1)
- 產品與檔案資訊
- 信任的發行者
- 信任的來源 SCCM
- 信任的軟體散發系統
- 信任的更新
- 信任的網路
- 信任的電腦映像
- 信任的 AD 群組
- 信任的產品

部署選項：

- Microsoft 群組原則 (GPO)
- 內部部署伺服器
- 軟體即服務 (SaaS)

附註：某些功能並非所有部署選項皆提供