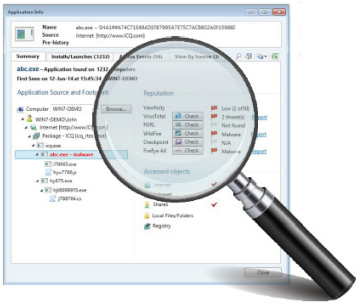
Viewfinity

有效將本機管理員特權最小化並管控端點及伺服器上的應用程式。



以單一頁面檢視所有的特權政策、應用程式和程式可信度。

面臨的挑戰

具本機管理員權限的帳號代表一個廣大且經常被利用的攻擊面，但若將業務用戶的管理權限全面移除的話則會導致不可預期的後果。當特權被剝奪後，組織可減少被攻擊面，但若業務用戶因而失去執行日常工作時所需的權限，伴隨著資訊安全優勢而來的，是以主要生產力作為代價的取捨。同樣地，針對 IT 管理員的特權政策通常是全有或全無的決策處置。其結果是，IT 管理員對伺服器經常會有不必要的完整管理權限，這樣會增加敏感伺服器的安全風險。甚至儘管組織已經盡一切努力使特權最小化以減少攻擊面，裝置本身仍可能會遭到惡意軟體的攻擊，而這些惡意軟體無需特權便可執行。

要有效減少攻擊面並減緩嚴重的數據洩漏而同時不影響到生產力，組織就應該要使用工具針對業務和行政用戶強制執行彈性化的最少特權政策，並管控哪些應用程式可以執行。若沒有這樣的工具，組織就會面臨下列的挑戰：

- **失去企業生產力。**當組織移除業務用戶所有的特權時，這些用戶可能就無法再執行某些工作或使用某些所需的應用程式以扮演其日常工作角色。其結果是，不具彈性的特權政策可導致企業運轉停頓。
- **高支援成本。**當 IT 政策阻礙業務用戶執行其日常工作時，這些使用者就必須呼叫服務台的支援以恢復所需的使用權限。這情況就會大幅增加 IT 的支援成本並使支援小組精疲力盡。
- **”特權蠕變”會增加安全風險。**當組織從業務用戶移除所有的特權時，IT 小組會不時地需要針對特定工作重新授予特權。然而，一旦特權被重新授予，就很少會被收回去。此"特權蠕動"的現象會再次因為過度的管理權限而開啟安全漏洞並使組織更容易受到威脅。
- **增加來自內部的和進階的威脅風險。**當組織以全有或全無的決策來處理 IT 管理員特權時，這些管理員最後卻會擁有遠多於所需的特權。若沒有制定以角色為基礎的特權政策，缺乏經驗的使用者就會很容易被惡意的內部人員或先進的攻擊者利用以取得未獲授權的帳號，並對敏感的系統進行破壞。
- **增加惡意軟體攻擊成功的風險。**組織即使盡可能減少 Windows 系統設備上的使用者特權，仍會受到無需特權就可執行的惡意軟體的威脅。若沒有最新的工具來管控哪些應用程式可以執行，攻擊者就可成功使用惡意軟體發動攻擊並取得在組織內的立足點。

解決方案

CyberArk Viewfinity 可讓組織對業務和行政用戶強制執行最少特權政策，並能控制應用程式以減少攻擊面，同時不會造成生產力停頓。此解決方案幫助組織從業務用戶收回每日例行性管理特權，但可依受信任應用軟體的需求來無縫地提升其管理特權。CyberArk Viewfinity 也能夠讓安全小組對 IT 管理員強制執行粒度的最少特權政策，幫助組織有效地在 Windows 伺服器上區隔工作責任。除了這些特權控制外，此解決方案亦提供應用程式管控功能，其設計用來管理和控制哪些應用程式可在端點和伺服器上執行並防止惡意軟體滲透系統環境。組織有了CyberArk Viewfinity，就可以：

為何需要CyberArk?

CyberArk是阻止網路攻擊的專家，能防止攻擊癱瘓企業。

Viewfinity

- **依據業務需求自動建立政策。**CyberArk Viewfinity依據受信任的來源(Trusted Sources)，如SCCM、軟體經銷商、更新程式和其它來源，自動建立應用程式管控及特權提升政策。

- **依據需求無縫提升業務用戶特權。**一旦從業務用戶移除本機管理員權限後，CyberArk Viewfinity會依據政策，針對受信任應用程式所提出之需求來無縫地提升其特權。

- **快速辨認並封鎖惡意軟體。**自動將未知應用程式與商業用途的黑名單資料庫例如VirusTotal和NSRL的內容做比對，以便快速辨認已知惡意軟體並更新組織全體政策，防止這些惡意軟體在組織環境中運作。

- **讓未知的應用程式在受限模式下安全地執行。**未知應用程式，係指未受信任但亦非已知的惡意軟體，可在受限模式(Restricted Mode)下執行。在此情況下，業務用戶可執行未知的應用程式，但這些應用程式不得存取企業資源、敏感資料或使用網際網路。

- **用威脅偵測工具提升整合以便分析未知的應用程式。**CyberArk Viewfinity可將未知的應用程式傳送到Check Point、FireEye 和Palo Alto Networks等威脅偵測解決方案以執行自動檔案分析。這些解決方案會回傳可靠度等級，讓 IT小組能夠據以決定是否要封鎖或准許這些應用程式存在於組織環境中。

- **辨識環境中所有的惡意軟體執行項目。**此解決方案在每個受保護的裝置上採用核心基礎代理程式，可立即在環境中找出一個惡意軟體所有的執行項目以及其來源出處。

優點

CyberArk Viewfinity 讓組織能夠在減少攻擊面的同時保持各用戶的生產力。此一解決方案讓組織能夠：

- **加速創造價值的進程。**
  使用受信任來源(Trusted Sources)來對組織內超過 90%的應用程式自動建立特權政策，將耗時的人力 IT工作量降至最低。

- **維持業務用戶的生產力但不會影響安全。**讓業務用戶能夠在沒有本機管理員特權的情況下安全地執行所需的未知應用程式以保持生產力。

- **降低來自內部的和進階的威脅風險。**以使用者角色作任務區分並對管理員特權作粒度管控，防止意外和故意行為損害重要的Windows伺服器。

- **減緩以惡意軟體為基礎的攻擊。**管控哪些應用程式可以執行以及應用程式可存取哪些資源，主動防止惡意軟體獲得在 IT 環境內的立足點。

- **有效提升現有投資的效益， 快速且精準地偵測威脅。**以Check Point、FireEye and Palo Alto Networks等解決方案分析並偵測潛在威脅，加速對未知應用程式的分析。

- **加速對威脅的應對。**清晰檢視 IT 環境中惡意軟體的出處及範圍，以便快速了解威脅的嚴重性並加快處理速度。

全面性的解決方案

CyberArk Viewfinity是CyberArk特權帳號資訊安全解決方案(Privileged Account Security Solution)的一部份。這是一個完整的解決方案，它被設計用來主動保護環境，防止進階攻擊利用管理員特權獲得機會存取企業核心區塊、竊取敏感資料和損毀重要系統。此解決方案刪除不需要的本機管理員特權並強化特權帳戶的安全，幫助組織減少攻擊面。

CyberArk特權帳號資訊安全解決方案針對實體和虛擬機器、資料庫、應用程式、虛擬監控程序、網路設備、安全設施和其它裝置上的特權帳戶進行主動保護、隔離、控制和持續性監控。此整體解決方案中的個別產品可以被獨立管理，或者合併成一個緊密結合且涵蓋廣泛的特權帳戶資訊安全解決方案。

規格說明

支援的平台：

Windows Desktop:

- Windows XP SP3
- Windows Vista SP1
- Windows 7 32-bit & 64-bit
- Windows 8 32-bit & 64-bit
- Windows 8.1 32-bit & 64-bit
- Windows 10

Windows 伺服器:

- Windows Server 2003 SP2 32-bit & 64-bit
- Windows Server 2008 32-bit & 64-bit
- Windows Server 2008 R2 64-bit
- Windows Server 2012
- Windows Server 2012 R2

全面性的應用程式支援：

- Executable
- MSI, MSU
- Administrative Tasks
- Management console snap-ins
- Scripts
- Registry settings
- ActiveX controls
- COM objects
- Web Applications

具彈性且安全的應用程式規則：

- File path matching
- Command line matching
- File hashing (SHA-1)
- Product and file information
- Trusted publisher
- Trusted Source SCCM
- Trusted Software Distribution system
- Trusted Updater
- Trusted Network
- Trusted Computer image
- Trusted AD group
- Trusted product

佈署選項：

- 群組原則物件 (GPO)
- 在組織內運行的伺服器 (On-premises server)
- 軟體即服務 (Software-as-a-Service)