CYBERARK®

白皮書

CyberArk 特權存取安全解決方案

業界最全方位解決方案，有效降低特權憑證及祕密資訊相關風險

www.cyberark.com/tw

目錄

特權存取 — 真實、無孔不入的威脅

攻擊者正在發起精心策劃複雜的進階網路攻擊，攻擊目標直接針對企業最重要的核心資產，因此在全球範圍內造成嚴重破壞。越來越多企業開始採用雲端優先策略並實施 DevOps 方法，這為攻擊者提供侵入未受保護企業的新途徑，擴大可攻擊的面向。攻擊者入侵後，會設法存取企業的核心系統，意圖造成重大損失，這可能包括聲譽受損、經濟損失及智慧財產權被盜，進而公開外洩機敏資訊或植入後門以近一步造成企業內部損害且曝光企業內部人士資料。Forrester 估計，80% 的安全性漏洞涉及特權憑證。[1]

特權帳號及特權帳號存取是目前企業面臨的最大資安隱患。為什麼企業內外的攻擊者會盯上特權帳號呢？

- 特權帳號無處不在，位於每一台網路設備、資料庫、應用程式、伺服器、雲端、DevOps Pipeline 及工控環境中
- 使用者及程式設定內使用的特權帳號擁有存取機密資料及系統的全面存取權
- 特權帳號擁有共用管理者存取權，允許使用者保持匿名存取
- 特權帳號擁有過於廣泛的存取權，這遠遠超出使用者執行其工作職能所需的權限
- 特權帳號不受監控並且不會被舉報，因此不安全

簡言之，只要擁有特權帳號，任何人都可以控制企業資源、停用安全系統並存取大量機敏資料。所有預測均表明，除非企業立即採取行動，否則，未來濫用特權帳號的情況會不斷惡化。最佳實踐指出，應將特權帳號納入企業的核心資安策略。特權帳號會引發資安問題，因此需要單獨對特權帳號實施控制，以保護、監控、偵測、告警並回應所有特權活動。

特權憑證 — 入侵 IT 王國的鑰匙

特權憑證是入侵 IT 王國的鑰匙。外部攻擊者及惡意內部人士會設法獲取特權憑證用於解鎖特權帳號，進而直接存取企業的核心資產。因此，企業關鍵系統及機敏資料的安全完全取決於存取這些資產所需的特權憑證。

當前，大多數企業都組合使用各種特權憑證，如密碼、API 金鑰、憑證、權杖及 SSH 金鑰，來對存取特權帳號的使用者及系統進行身份驗證。如果未受到有效保護，攻擊者就可以攻破這些重要的祕密資訊、佔有特權帳號，並利用這些祕密資訊向企業發起攻擊。事實上，網路安全調查表明，每名攻擊者要想成功發動攻擊，先決條件就是存取特權帳號。尤其值得一提的是，由於一些企業已經開始保護特權密碼，攻擊者已將攻擊目標轉向 SSH 金鑰，因為企業在保護特權帳號時，常常忽略這類金鑰。

為防範有針對性的攻擊、保護入侵 IT 王國的鑰匙並使攻擊者無法竊取機敏資料，企業必須採用特權存取安全策略，在策略上主動納入保護並監控所有特權祕密資訊及憑證。

向專家學習：CyberArk 特權存取安全

CyberArk 是特權存取安全領域的市佔率領導者及可信賴的專家。在保障特權存取安全方面，我們的豐富經驗優於任何其他廠商；我們充分利用這方面的專業知識，運用清晰有效的方法協助客戶管理特權存取相關風險。

為降低重大資料外洩的風險，企業需要採用資安解決方案來專門應對其面臨的特權存取風險。CyberArk 的特權存取安全解決方案將提供所需的全面保護、監控、偵測、告警及報表功能，協助企業領先攻擊者掌握先機，保護企業最關鍵的資產。

[1] The Forrester Wave™：特權身份管理，2018 年第 3 季

您是否低估自己面臨的風險等級？

在《2018 年 CyberArk 威脅趨勢報告》[2] 中，我們發現，89% 的 IT 資安專業人士認識到，除非有效管理及保護特權帳號、憑證及祕密資訊，否則將無法全面保護基礎架構及關鍵資料。但是，有相當一部分資安專業人士指出，他們任職的企業仍未實施特權存取安全解決方案來儲存及管理特權帳號密碼。而且，2018 年報告表明，企業未採取足夠有效的措施來防範惡意軟體及進階攻擊，但是，87% 的受訪者表示，他們仍允許使用者擁有本機管理者權限，眾所周知，大多數惡意軟體需要管理者權限才能持續運行。結合擁有本機管理者權限的使用者帳號與實際的管理者帳號，就可以進一步擴大特權帳號的攻擊面。

此外，DevOps 安全性尚未達到傳統企業 IT 的成熟水準。一半的受訪者未針對雲端或 DevOps 實施特權安全策略，近 40% 的受訪者將特權帳號密碼及祕密資訊儲存在簡單的文字檔中，意謂未有效管理及保護高價值帳號，導致整個環境面臨極大風險。考慮到典型企業由於 [缺乏] 特權存取安全而面臨的所有這些風險，鑒於過去 8 年中 80% 以上的資安攻擊在一定程度上都成功利用特權帳號，顯而易見，IT 資安專業人士需要在特權帳號領域制定專門的攻擊防範計畫。

法規遵循生死攸關

由於進階威脅的風險與日俱增，PCI DSS、Sarbanes Oxley、NIST、NERC-CIP、HIPAA、GDPR 等法規遵循條例以及 SWIFT CSCF 之類的框架都增加對於控制、管理及監控特權存取的規定。

未充分瞭解其特權環境的企業將面臨稽核缺失而必須付出高額罰款及接受處罰，更為重要的是，由於未制定特權存取安全策略，企業本身仍然易於受到可怕的攻擊。

誰是您的特權使用者？

企業傾向於忽視大量存取特權帳號的情況。企業僅制定少數資安或稽核原則來控制與特權帳號相關的風險。匿名、未經檢查地存取這些帳號會使企業面臨帳號濫用風險，如果帳號被攻破，企業可能會遭受嚴重後果。

遠端廠商：向承包商授予特權存取權以執行工作職能，使承包商在匿名狀態下工作。一旦系統遭到入侵，遠端廠商就像任何「標準」特權使用者一樣擁有不受限制的存取權，並且可以提權以存取整個企業的機敏資料。

虛擬環境或雲端平台管理者：財務、HR 及採購等業務流程正逐步轉移到雲端應用程式中，由於雲端管理者被授予廣泛的存取權，企業資產將面臨較高風險。

系統管理者：IT 環境中的幾乎每台設備 (每個終端設備及伺服器) 都有一個共用特權帳號，該帳號原生具有特權並且可以不受約束地存取作業系統、網路、伺服器及資料庫。

應用程式或資料庫管理者：應用程式及資料庫管理者被授權廣泛的存取權，以便管理分配給他們的系統。利用這種存取權，他們還可以連接企業內部的幾乎任何其他資料庫或應用程式。

某些企業使用者：資深管理人員及 IT 人員通常擁有特權存取權，可以存取保存有機敏資料的企業應用程式。如果落入惡意人員手中，這些憑證可用於存取財務資料、智慧財產權及其他機敏資料。

終端使用者：有許多公司仍然允許終端使用者擁有本機管理者存取權，執行安裝軟體及設定印表機等操作。如果惡意人員取得本機管理者存取權，這些特權憑證可為入侵的攻擊者提供第一個「駐留點」，然後開始竊取財務資料、智慧財產權及其他機敏資料。

[2] CyberArk，《CyberArk 2018 年全球進階威脅趨勢調查報告》，2018 年

社交媒體：為管理企業內部及外部的社交媒體，會授予特權存取權給相關人員。員工及承包商會被授予特權存取權，以在社交媒體帳號中編寫內容。濫用這些憑證可能會導致帳號被公開接管，造成企業的品牌或高階主管的聲譽受損。

應用程式：應用程式使用特權帳號來與其他應用程式、腳本、資料庫、Web 服務等進行通訊。這些帳號通常被忽略，因而存在重大風險，因為這些帳號往往是採用寫死的靜態憑證。駭客可以利用這些攻擊點來提升在整個企業內部的特權存取權。

DevOps：利用 DevOps Pipeline，企業可以自動建構並部署服務及應用程式，實現較高的敏捷性。為存取資料以及其他應用程式與服務，這些服務需要取得受到嚴密保護的祕密資訊及其他憑證。此外，一些強大工具支援典型的 DevOps Pipeline，每個此類工具的管理主控台都由其管理者進行管理，而這些管理者帳密憑證也必須受到保護。

原則優先：風險管理與業務目標相得益彰

最佳實踐建議，企業應制定、實施並執行特權存取安全性原則，以降低嚴重資料外洩的風險。為有效保障企業安全性及法規遵循，首先應執行適當的業務原則。原則優先方法可確保降低外部威脅、內部人士威脅及濫用風險，並遵循嚴格的政府及業界法規遵循條例。

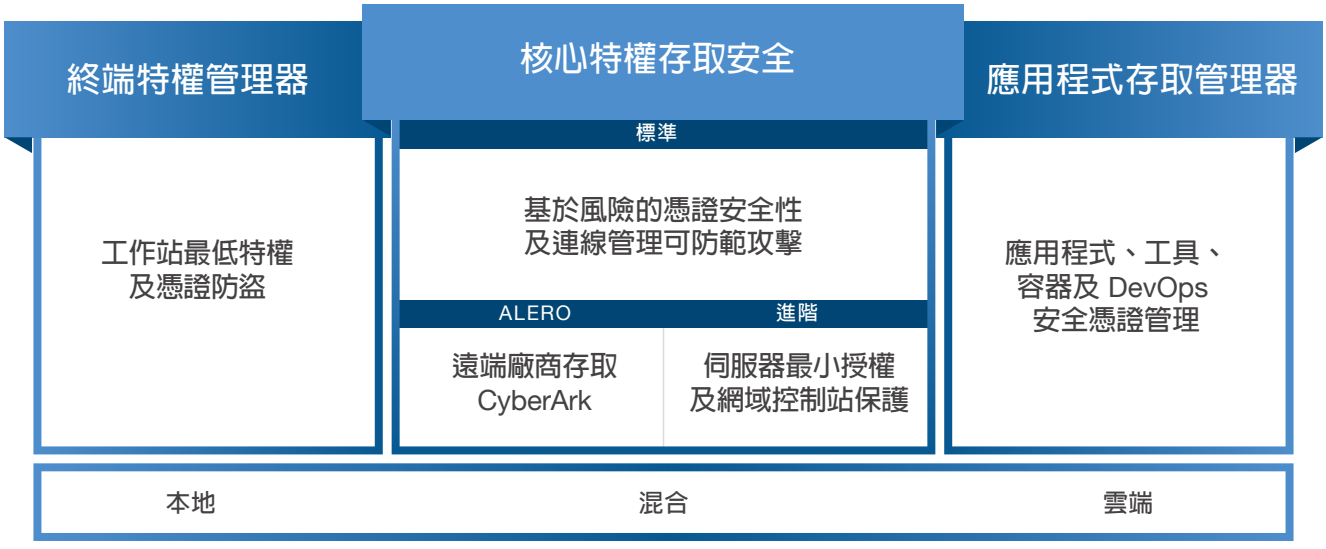
CyberArk 共用技術平台

CyberArk 在設計之初就旨在確保特權存取安全，組合強大的底層基礎架構與我們的核心產品，可為任何規模的企業提供最全方位解決方案。

該基礎架構的核心包括隔離式金庫伺服器、統一的規則引擎、探勘引擎及多個安全層，可為特權存取提供可延展性、可靠性及無與倫比的安全性。靈活的架構可從小規模開始，然後擴展為規模最大、要求最嚴苛的企業部署。

唯有 CyberArk 有能力提供各種解決方案，協助保護、管理並稽核使用者及應用程式憑證，落實最小權限存取，管控終端設備及伺服器上的應用程式，同時保護、監控並分析所有特權活動，進而在發現異常行為時主動告警。此全方位企業級解決方案旨在保護、監控、偵測及回應特權活動，防篡改、可擴展、專為複雜分散式環境而設計，提供最高安全性，進而防範內部及進階威脅。

CyberArk 特權存取安全解決方案



主要原則 (Master Policy™) — 以簡化、統一、無與倫比的方式設定原則優先順序

主要原則 (Master Policy) 是一種創新的原則引擎，使客戶可以使用簡單的自然語言介面設定、管理並監控特權存取安全性原則。將業務原則及流程轉變為技術設定的過程曾經非常複雜；而現在此過程對企業相關人員 (包括資安、風控及稽核團隊) 來說變得非常易於管理及理解。主要原則位於核心系統中，且功能跨越整個 CyberArk 特權存取安全解決方案，提供簡化、統一而無與倫比的原則管理。

主要原則會將以自然語言編寫的安全性原則對應為技術設定，並管理此項原則。現在即可在數分鐘內實施特權存取安全控制措施，從而提高流程的等級，如果不使用主要原則，可能需要數天甚至數周時間實施。主要原則可協助快速實施並靈活制定全企業原則，同時提供受控制、精細的特殊原則來滿足作業系統、地區、部門或業務線的獨特運營需求。

數位金庫 (Digital Vault™)

廣受好評、專利設計的數位金庫 (Digital Vault™) 是一種經過強化的隔離式伺服器，採用 FIPS 140-2 加密的金庫專屬通訊協定。為確保完整性，所有 CyberArk 產品將直接與金庫進行互動並共用資料，以便所有產品模組及元件進行可靠通信，存在於本地、混合及雲端環境的密碼、SSH 金鑰、原則設定及稽核日誌亦使用階層式加密安全地儲存。

- **職責分離及強大的存取控制：**金庫管理者無權存取儲存在金庫中的帳密憑證，這確保適當的職責分離。此解決方案支援多種身份驗證方法，可確保安全性並控制所有特權憑證存取及活動。
- **安全層：**七個內建安全層用於身份驗證、存取控制、加密、防篡改儲存及資料保護，並且沒有後門或 DBA 存取權，這實現極高的安全性。
- **高可用性及災難恢復：**此基礎架構旨在實現高可用性，並內建自動防故障功能，可按預期甚至超預期滿足災難復原的要求，包括安全的備份及簡單的復原作業，因此，將不會出現任何單一故障。

探勘引擎

此探勘引擎旨在持續發現 IT 環境 (無論在雲端還是本地) 的變化情況，可提供最新的保護功能，並協助監控並保護所有特權活動。新增或刪除新伺服器及工作站時，會自動找出特權帳號的變更情況。

安全稽核

CyberArk 的特權存取安全解決方案將自動實特權帳號原則、實現持續監控，進而滿足稽核要求。IT 稽核團隊不僅能夠全面瞭解所有特權連線期間的相關「人員、時間及原因」，而且瞭解具體發生「什麼」。該解決方案運用所有稽核資料的單一、集中式儲存庫，提供簡化、具成本效率的稽核報告功能。

企業級整合

特權存取安全解決方案可運用 REST API 提供的廣泛自動化支援，輕鬆整合您現有的資安、維運及 DevOp 工具。

- SIEM：與 SIEM 廠商的全面雙向整合提高威脅偵測及告警能力。CyberArk 會將有關特權憑證存取及維運的事件發送到 SIEM 解決方案，並發送運用特權連線監控功能所捕獲的指令操作。
- **混合雲：**對混合雲端環境的支援可協助保護虛擬及雲端管理者與客體中的帳號，保護 Amazon Web Services、Microsoft Azure 及 Google Cloud Platform 中的特權帳號。
- **弱點掃描：**全面整合領先的弱點掃描廠商有助於他們簡化「需經過身份驗證的掃描」(也稱為「深度掃描」)，並在任何時候需要登入到目標伺服器以執行掃描時提取特權帳號。
- **身份管理：**整合領先的身份及存取管理 (IAM) 解決方案，以根據目錄詳細資訊、群組成員資格或身份治理原則將帳號設定到解決方案中。此外，整合還有助於我們的客戶利用以前在身份驗證方面的投資，如 PKI、Radius、Web-SSO、LDAP 等。

- **服務台：**整合大多數企業工單系統以及內部解決方案。功能包括服務請求驗證、建立新服務請求以及整合稽核工作流程，如管理者覆核（雙重控制）及存取時間。
- **DevOps：**與 DevOps 工具鏈的整合可協助保護及管理 Ansible、Chef、Jenkins 及 Puppet 等 CI/CD 工具與 Docker 等容器協作軟體所使用的祕密資訊。

可擴展、靈活小巧的架構

CyberArk 的特權存取安全解決方案旨在最大幅度降低影響並保護您當前 IT 環境中的現有投資。所有組件均獨立運行，但利用共用資源及資料。透過這種靈活的方法，企業可以在部門級別開始啟動專案，然後隨著時間的推移將其擴展為複雜的分散式企業解決方案。

CyberArk 產品

CyberArk 特權存取安全解決方案中包含的每一種產品都是獨立的，可以獨立進行管理，同時可共用來自通用基礎架構的資源及資料。

每款產品都滿足特權存取安全方面不同的需求，所有產品設計為可協同工作，運用 DevOps Pipeline，為本地、雲端及工控安全環境中的作業系統、終端設備、伺服器、資料庫、應用程式、虛擬機、網路設備、資安設備等提供全方位安全解決方案。

保護特權存取的建議步驟：

- 設定原則優先順序。
- 清查所有特權帳號及憑證。
- 保護並管理使用者及應用程式使用的特權帳號密碼。
- 控制、保護並監控對伺服器及資料庫、網站、SaaS 以及任何應用程式的特權存取。
- 為企業使用者及 IT 管理者提供最小存取權。
- 管控終端設備及伺服器上的應用程式。
- 利用即時特權帳號情報來偵測並回應發生中的攻擊。

核心特權存取安全

帳密憑證保護及管理

清查、管理及保護特權憑證

CyberArk 解決方案將阻止對特權使用者密碼及 SSH 金鑰的惡意使用，同時整理並保護易受攻擊的帳號。CyberArk 解決方案會根據特權存取安全性原則來全面保護特權憑證，控制誰可以在什麼時候存取哪些憑證。這種自動化流程可以減少手動追蹤及更新特權憑證時耗時而容易出錯的任務，輕鬆滿足稽核及法規遵循標準。

- 阻止未授權使用者存取特權帳號憑證，並確保授權使用者擁有執行合法商業活動所需的存取權。
- 根據原則定期或依需求更新並同步特權密碼及 SSH 金鑰。
- 清查並保護本地、混合及雲端環境，整個 DevOps Pipeline 以及外部網路偶而連網的終端設備中所使用的特權憑證。
- 協助使用者運用 REST API 自動完成並簡化特權帳號管理任務，如帳號工作流程、啟用規則、權限授予等。
- 協助資安及稽核團隊清楚瞭解哪些使用者何時出於什麼原因存取哪些特權帳號或共用帳號。

連線隔離及監控

隔離、控制及即時連線監控與記錄

CyberArk 解決方案將保護、隔離、監控 Unix、Linux 及 Windows 的關鍵系統、資料庫、虛擬機器、網路設備、大型主機、網站、SaaS 等的特權使用者存取及活動。CyberArk 解決方案將提供單一存取控制點，透過隔離終端使用者，有助於防止惡意軟體侵入目標系統，並記錄每次按鍵操作及滑鼠點選以實現持續監控。

DVR 式錄影提供連線的完整視圖，並設定機敏事件相關的搜尋、定位及告警功能，而不必利用日誌進行篩選。即時監控有助於持續保護特權存取，而且，如果認為任何可疑活動存在，就可以自動暫停及終止特權連線。此外，CyberArk 解決方案還全面整合協力廠商 SIEM 解決方案，可發出異常活動告警。

- 隔離特權連線，以防止惡意軟體從使用者的終端設備擴散到關鍵系統。
- 協助保護特權密碼及 SSH 金鑰，防止按鍵輸入記錄及雜湊傳遞等進階攻擊手段。
- 保護並控制特權連線，防止惡意軟體或零時差漏洞繞開控制措施。
- 建立防篡改特權連線記錄並提供可搜尋的中繼資料。
- 提供指令控制及本地 SSH 存取，同時仍然提供使用者使用密碼或 SSH 金鑰進行特權安全存取。
- 提供 AD Bridge 功能，協助企業集中管理透過 CyberArk 平台連結到 AD 的 Unix 使用者及帳號。

特權分析及威脅偵測

分析惡意特權活動並發送告警

CyberArk 提供安全智慧解決方案，可協助企業偵測正在進行攻擊的反常特權活動、發送告警並做出回應。CyberArk 解決方案會從多個來源 (包括 CyberArk 數位金庫、SIEM 及網路封包) 收集一組特定資料，然後，CyberArk 解決方案會應用一組複雜的統計學確定性演算法，確定惡意特權活動，協助企業在攻擊生命週期的早期階段偵測入侵跡象。

- 進行即時偵測並發送告警，自動回應偵測到的事件。
- 確定與特權存取有關的異常行為及惡意活動，能夠偵測進行中的攻擊。
- 利用自我學習演算法，使威脅偵測適應不斷變化的風險環境。
- 關聯各種事件並指定威脅等級。
- 利用現成可用的整合提升現有 SIEM 解決方案的價值。
- 運用有關使用者模式及活動的資訊性資料改進稽核流程。

Alero™：遠端廠商存取

協助遠端廠商安全快速地連接到 CyberArk，無需 VPN、代理程式或密碼

CyberArk® Alero™ 是一種 SaaS 解決方案，結合零信任存取、生物辨識身份驗證與即時供裝功能。運用完全整合 CyberArk 核心特權存取安全解決方案以提供全面的稽核、記錄及補救功能，Alero 確保遠端廠商只擁有所需的存取權。Alero 旨在為需要存取關鍵內部系統的遠端廠商提供快捷、方便且安全的特權存取。

由於不需要 VPN、代理程式或密碼，Alero 降低管理者的維運成本，提高企業安全性。

- 整合 CyberArk 核心 PAS，可為關鍵系統提供另一層安全保護
- 引入比基於權杖或 VPN 傳統方法更加安全的解決方案
- 降低與管理 VPN、代理程式及密碼相關的維運成本

最小授權管理

為 UNIX/Linux 及 Windows 伺服器提供精細控制

CyberArk 允許特權使用者在原生 Unix 或 Linux 連線中使用管理指令，同時移除不必要的 root 存取或管理者權限。這個與 sudo 類似的企業級資安解決方案集中且相互關聯勹所有超級使用的者活動的日誌記錄並且將其連結到個人使用者名稱，同時提供執行工作職能所需的自由性。在提供精細存取控制同時，持續監控超級使用者基於其角色及任務執行的所有管理指令。此解決方案還可協助企業阻止及遏制對 Windows 伺服器的攻擊，以降低資訊被盜或被加密勒索的風險。

- 用提供精細特權控制並安全儲存稽核日誌的集中式備選方案替代常用的 sudo 解決方案。
- 向稽核人員提供超級使用者特權受保護、受管理及受控制的證據。
- 提供詳細的稽核記錄，說明哪些個人什麼時候出於什麼原因將權限提高到 root 權限。
- 僅授予超級使用者特權給向必要人員，以降低濫用或出錯風險。
- 向使用者授予全面的 root shell 的存取權，以根據他們的工作流程直觀地完成工作。
- 現成的原則範本可基於使用者角色控制管理者特權，協助在 Windows 伺服器上實現責任分離。
- 基於使用者及系統將指令加入白名單 / 黑名單。

網域控制站保護

保護 Windows 網域控制站，防範 Kerberos 攻擊

CyberArk 提供超輕量級 Windows 代理程式，可執行網路行為分析來偵測進行中的 Kerberos 攻擊。此解決方案會監控並保護網域控制站，阻止假冒及未授權存取。此解決方案有助於防範一系列常見的 Kerberos 攻擊手段。

- 偵測一系列潛在的威脅，包括疑似憑證盜竊、橫向移動及提權。
- 透過 CyberArk 控制台、電子郵件或 SIEM 控制台提供即時告警。
- 能夠在網域控制站上實施精細控制（以實現最小授權）及應用程式控制。
- 偵測一系列進行中的 Kerberos 攻擊，包括 Golden Ticket、Overpass-the-Hash 及 PAC 操作。

應用程式、容器及 DevOps 祕密資訊管理

應用程式存取管理器（Application Access Manager™ ）

保護、管理並稽核本地、混合雲、容器化以及多雲端環境中的應用程式憑證

CyberArk 應用程式存取管理器（Application Access Manager）旨在為廣泛使用的各種應用程式及內嵌身份提供全面的特權存取、憑證及祕密資訊管理。例如，應用程式存取管理器可保護商用套裝應用程式、內部開發的傳統應用程式、腳本以及使用 DevOps 方法建構的容器化應用程式所需的憑證。

應用程式存取管理器旨在提供強大的安全解決方案，協助企業控制、管理並稽核本地、混合雲、容器化及多雲端環境中的各種應用程式所需的所有內嵌特權存取。

- **建立嚴格的身份驗證** — 利用應用程式、容器及其他內嵌身份的原生屬性應對「祕密資訊零引導」（secret zero bootstrapping）挑戰並消除潛在的漏洞。
- **簡化整合** — 經過驗證，支援整合一系列商用軟體平台、應用程式及工具，如業務應用程式、資安工具、RPA 平台、CI/CD 工具集及容器平台。
- **加速開發及使用** — 為開發人員提供易於使用的解決方案來保護應用程式及 DevOps 環境中的祕密資訊 — 便於他們集中精力開發軟體。此外，利用開源解決方案，開發人員及 DevOps 管理者可以輕鬆評估、部署 DevOps 環境並確保其安全。
- **確保全面稽核任何存取** — 追蹤所有存取並提供防篡改稽核記錄。

- **一致地應用存取原則** — 對內嵌身份應用基於角色的存取控制，利用與其他 CyberArk 及合作夥伴解決方案的整合在整個企業內部進行集中化原則管理，並實施其他基於原則的控制。
- **確保業務連續性並滿足其他企業要求** — 包括可延展性、可用性、冗餘及彈性、告警、基於原則的更換及其他要求。

終端設備特權管理及憑證防盜

終端設備特權管理器

在終端設備上實施最小授權

終端設備特權管理器可保護終端設備 (Windows 及 Mac 桌上型電腦 / 筆記型電腦) 上的特權並在生命週期的早期防止攻擊擴散。終端設備特權管理器能夠協助撤銷本機管理者權限，同時藉由無縫提升已授權應用程式或任務的權限，最大幅度降低使用者生產力受到的影響。運用自動制定原則可以實施應用程式控制，這便於企業防止執行惡意應用程式，並在受限模式下運行未知應用程式。這與憑證防盜結合，有助於防止惡意軟體入侵，並阻止在終端設備上實施的攻擊。

- 協助企業取消日常企業使用者的本機管理者權限，而不影響生產力，並在需要時根據原則無縫提權，以執行已授權應用程式或指令。
- 防止惡意應用程式 (包括勒索病毒) 入侵並在整個環境中擴散，並允許使用者以「受限模式」執行未知應用程式，協助使用者保有生產力並確保安全。
- 協助企業偵測並阻止企圖竊取 Windows 憑證及常用網路瀏覽器儲存的憑證的行為，防止其通過環境傳播。
- 全面整合 CyberArk 應用程式風險分析服務，可自動分析未知應用程式並及時做出原則決策。
- 無縫整合 Check Point、FireEye 及 Palo Alto Networks 威脅偵測解決方案。

關於 CyberArk

CyberArk 是特權存取安全領域的全球領導者，特權存取安全是在整個企業、雲端及 DevOps Pipeline 內保護資料、基礎架構及資產的 IT 安全性的關鍵領域。CyberArk 提供業界最全方位解決方案，可降低特權憑證及祕密資訊引發的資安風險。公司深得全世界領先企業的信賴，包括 50% 以上的財富 100 大公司。這些公司利用 CyberArk 產品來防止外部攻擊者及心懷惡意的內部使用者發起攻擊。CyberArk 是一家全球性公司，總部設在以色列 Petach Tikva，美國總部位於麻塞諸塞州 Newton。公司在美洲、EMEA、亞太地區及日本皆設有辦事處。

有關 CyberArk 的更多資訊，請存取 www.cyberark.com/tw。