BeyondTrust

UNIX 與 LINUX 特權管理

保護特權帳戶並達到合規性

BeyondTrust Unix 與 Linux 特權管理為最高標準的企業級特權管理解決方案，可提供無法比擬的高可見性，並有效控制複雜伺服器環境。

特色與功能

- **稽核與控管：**蒐集與安全儲存按鍵輸入記錄、工作階段記錄及其他特權事件，並將其編入索引，即可分析使用者行為。
- **細緻的最低特權：**藉由細緻的原則型控制功能，提高標準使用者在 Unix 和 Linux 上的特權。
- **動態存取原則：**利用時間、日期、位置與應用程式/資產弱點狀態等因素來制定提高特權的決策。
- **遠端系統與應用程式控制：**可讓使用者執行特定命令，並根據規則遠端執行工作階段，無須以管理員或根使用者身分登入。
- **檔案與原則完整性監控：**針對重要原則、系統、應用程式及資料檔案的變更進行稽核與報告。
- **特權威脅分析：**透過最佳安全性解決方案，讓使用者行為可與資產弱點資料及安全情報相互關聯。

限制根存取

提供細緻的特權提高規則，以單獨執行特定工作或命令。

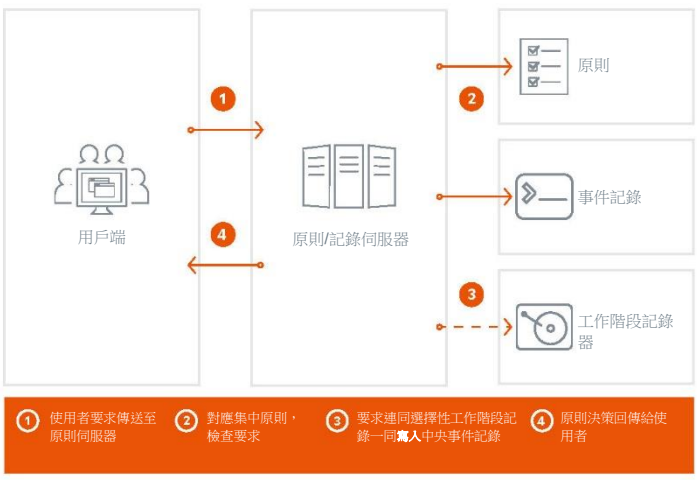
稽核所有使用者活動

保護檔案、指令碼與目錄不會受到未經授權的變更。

監控記錄與工作階段

即時偵測可疑的使用者、帳戶與資產活動。

運作方式



支援平台

BeyondTrust Unix 與 Linux 特權管理支援超過 100 個平台，包括 Debian GNU、HP-UX、HP Tru 64、Red Hat Enterprise Linux、Sun Solaris、SuSE Linux Enterprise、VMware ESX、IBM AIX 及其他項目。

「Unix 與 Linux 特權管理在實作上取得極大成功，能夠限制所有伺服器存取，甚至是經由 SSH 執行的存取。稽核者可輕鬆檢視追蹤中的程序，而我們的 IT 人員也能維持一貫的生產力。」

SVP SYSTEMS/RECOVERY、CTO、DCI

商業優勢

確保合規性

- 提供所有使用者活動的完整稽核記錄。
- 劃分需使用特權帳戶的 IT 工作，確保符合法規。
- 確保重要檔案及原則未遭到竄改。

保障重要系統與檔案安全

- 僅提供完成工作所需的存取權限，藉此限制受攻擊面。
- 避免使用根帳戶。
- 僅能執行核准的應用程式/命令。
- 消除可能導致遭到入侵的因應措施或漏洞。
- 根據內容與風險制定特權決策。
- 避免重要檔案遭惡意程式攻擊及誤用。

提高效率

- 精簡使用 sudo 時需執行的複雜處理程序。
- 簡化使用集中式管理主控台時的管理與速度部署。

在特殊權限存取管理的領域中，BeyondTrust 始終獨步全球，提供最出色的無縫解決方案，防範因權限管理不當而導致的資料外洩。隨著威脅範圍逐漸擴及端點、伺服器、雲端、DevOps 及網路裝置環境，我們的可延伸平台能有效協助各組織輕鬆升級權限安全性。至今為止，我們深受 20,000 多位客戶信任。

beyondtrust.com