Linux 端點權限管理
最小權限並簡化合規性

挑戰

Linux 系統提供組織關鍵性的業務操作，支援重要的服務、儲存敏感的數據。然而，許多組織缺乏健全的安全措施來保護這些高價值的端點。因此，Linux 用戶可能會被賦予過大的 root 存取權限，而這種存取權限容易造成監控和稽核上的管理問題。

從 2022 年到 2023 年，Linux 勒索病毒攻擊增加了 62%[1]。

資安的威脅分為外部與內部威脅。內部人員同樣可能帶來風險，無論是故意濫用其權限，還是無意中犯錯，都可能會危及關鍵系統或敏感的數據。

組織需要具備完整的可視性和適當的解決方案來管理 root 存取權限並監控 Linux 用戶的特權活動，並在必要時進行稽核與回應，以維持合規性、取得網路防護及追蹤關鍵業務的端點變更。

- **如何在不影響使用者效能，控制 root 存限權限以實現最小特權管理？**
- **如何集中收集特權事件日誌和會話錄製，以簡化合規性？**
- **如何集中管理 Linux 環境的零信任安全控制？**
- **如何產生報告以了解用戶在 Linux 環境中的權限？**

許多組織嘗試使用像 sudo 這樣的開源工具來管理 Linux 環境中的特權存取。儘管 sudo 可以提供一定程度的特權存取管理，但它遠遠不足以滿足現代企業 Linux 部署所需的進階的特權管理和稽核要求。

利用 sudo 管理 root 訪問對 IT 和資安團隊來說可能是一個繁瑣且人力密集的過程，隨著組織的部署變得更大和更複雜，這一過程的困難只會增加。由於缺乏有效的集中管理、潛在的合規性問題，以及不支援不可變的稽核或會話錄製，顯然 sudo 的諸多不足對大多數的組織來說成為一個不適切的特權管理解決方案。

解決方案

BeyondTrust Linux 端點特權管理是一個企業級的特權提升和委派管理解決方案，使客戶能夠控制 root 存取、簡化合規性、強制執行最小特權，並集中管理零信任安全控制，且不影響生產力。這款專為 Linux 設計的解決方案使客戶能夠通過集中事件記錄、會話監控和管理，以及子進程控制，擴展功能，遠超過 sudo。該解決方案，部署簡單且能快速擴展。

Linux 端點特權管理的概念是在1990 年代初由麻省理工學院和美國國防部頂尖的數據科學家的工程師們所提出。到 1994 年，全球的大型銀行已經將該解決方案標準化。

[1]The Linux Threat Landscape Report. Trend Micro. August 2023.

具備市場上最大的安裝基礎，Linux 端點特權管理是最可靠和最值得信賴的特權管理解決方案。現今，客戶包括：

- 全球的大型銀行
- 涵蓋美國、南美洲、亞洲和中東的電信龍頭
- 聯邦、州和地方政府機構
- 數百家中小型組織

主要特性與功能

細緻最小特權
透過精細的政策控制來控制 root 存取，並動態提升標準用戶的特權，取代 sudo，消除對 root 會話的需求。

強大的稽核簡化合規性
集中蒐集和管理日誌事件，包括特權提升事件的日誌和完整會話錄製。日誌以安全、不可變的格式儲存。

依角色的政策控制
通過輕量級且易於實施的角色的政策快速解決核心安全漏洞，這些政策可以根據「誰、什麼、在哪裡、何時」來建立。

集中管理
集中管理您的 Linux 環境，包括所有用戶活動數據、政策、升級、更新和部署。

整合與延展性
與其他系統和工具（如 SIEM、Elasticsearch 或 BeyondTrust Active Directory Bridge）整合，擴展您混合環境中的身份驗證功能。

優勢

強化 Linux 安全性
根據靈活的角色或腳本的政策動態提升標準用戶的特權，限制攻擊面，並防止使用 root 帳戶。

簡化合規性與網路防護
提供所有用戶活動不可異動的稽核記錄，確保遵循日益複雜的法規並符合網路防護的要求。

監控與追蹤所有特權活動
全面集中監視所有特權用戶的活動，包括完整的會話錄製，進而提高變更信任並改善事件回應時間。

提高營運效率
簡化可能與 sudo 或自定義工具相關的複雜過程，來精簡管理和運營，並提升用戶生產力。