

特權遠端連線安全

管控和審核員工與供應商間的遠端連線存取

當今的企業需要有效管理不斷擴大且複雜的網路範圍，網路現況包括基礎架構即服務 (IaaS)、內部雲端資源及網頁管理平台，供應商和員工需要遠端連線處理問題，不適當的遠端連線，如私人虛擬網路 (VPN) 是存在較高風險，也易成為駭客的攻擊途徑。

BeyondTrust 特權遠端連線安全提供可視性，管控所有遠端存取，包括 IT 管理人員、第三方供應商、開發人員及 **CloudOps** 工程師，確保適當的人在合適的時間存取正確的系統，企業採用這個解決方案，能同時滿足嚴格的法規要求與安全。

「以前我們讓供應商遠端存取的唯一方法是建立 VPN，有了 **BeyondTrust**，我們可以限制他們的存取權限，並記錄他們的操作過程，因此我們能夠確切記錄所有行為的日誌，這讓我們的環境更加安全。」 - 北卡羅來納大學夏洛特分校商業與技術分析師

Brian Bard

功能特色：

管控特權存取

依照角色精細的控管存取和會話參數，清除了「擁有使用權限或無使用權限」的遠端存取無論是 Windows 伺服器還是 Kubernetes 集群，使員工和第三方能夠安全無縫地連接到任何地方的資產。

基礎設施即代碼 (Infrastructure as Code)

藉由易於使用的 API 和工具，善用自動化的優勢，輕鬆建立和移除雲端基礎設施，以及提供和收回存取權限，如 Terraform。

可攜電子設備 (BYOT)

提供技術人員安全的工作流程，無需使用 VPN，允許他們使用熟悉的工具，如 Putty、Azure Data Studio 執行工作。

輕鬆整合

建立一站式服務，將特權遠端連線安全與現有的 SIEM 整合，提供分析師和技術人員在他們的工作流程中使用。

特權遠端連線安全產品詳細資訊與展示

beyondtrust.com/remote-access

提升效率

提供安全的存取並保持順暢的整合，以不影響安全或合規性的工作流程。

滿足法規要求

記錄所有遠端支援活動會話日誌，集中儲存在一個中央資料庫中，簡化審核流程。

降低成本

減少 VPN 的需求，提升網路安全性，實現價值最大化。

