保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

守護關鍵基礎設施--為何傳統系統仍然很重要

2025 年 9 月 2 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

現代資訊科技 (IT) 不可或缺的隱形骨幹

在雲端原生應用程式、容器化工作負載與 AI 分析工具主導當今 IT 的焦點技術背後，存在著更為低調卻同樣關鍵的基礎架構：UNIX 與 Windows 這類傳統的企業系統。實際上從金融、醫療到製造業及政府部門，這些系統始終是經營運作的核心樞紐。它們承載核心銀行應用程式、管理醫療資料、交易處理系統、儲存戶籍謄本等公民個人資料--這些功能絕非能輕易在一夜之間就宣告終止支援。

事實上，儘管科技創新一路往前飛奔，大型企業仍高度依賴傳統的 Windows 與 Unix 系統來確保穩定性、合規性與可靠性。保護這些系統不僅關乎回溯相容性，更是守護企業營運基礎架構的關鍵所在。

為何傳統系統依舊持續在關鍵性任務有關的重要系統扮演重要角色

- 核心業務工作負載：銀行系統仍仰賴大型主機與 Unix 交易處理器執行高吞吐量、低延遲作業。航空公司透過過去數十年來通過高韌性考驗的傳統系統來調度機隊。
- 合規完善度與監管：醫療與金融產業面臨嚴格規範。傳統系統常儲存稽核與合規所需的病歷紀錄或交易檔案。
- 經長久驗證過的企業擴展成長所需之可靠性：傳統 Unix 系統專注於穩定性與業務持續正常運作時間 (Uptime) 的優化。對許多跨國企業而言，使用三十年的核心系統仍比全新的雲端原生應用程式更值得信賴。

這些平台不僅未退流行，反而已轉化為值得傳承的資產--而非負債。

系統終止支援的挑戰：刻不容緩的漏洞危機

隨著 Windows Server 2012 等傳統平台進入終止支援 (EOL) 的現實階段，企業面臨嚴峻挑戰：供應商不再發布修補程式，官方支援全面終止。然而，由於極度依賴這些系統，不得讓許多具漏洞風險的系統仍持續運作於生產環境中。

這幾年的重大資安事件的前車之鑑歷歷在目，沒有加裝任何保護措施的已終止支援系統總是成為首要的攻擊目標：

- WannaCry (2017年) 利用未修補漏洞的 Windows Server 2003/2008 系統，導致全球醫療與物流業的癱瘓。
- BlueKeep (2019年) 使數百萬未修補的 Windows Server 2008 及 XP 系統暴露於遠端程式碼執行風險。
- PrintNightmare (2021年) 凸顯 Windows 環境中長期存在的元件仍具高度吸引力。

若缺乏主動式防護機制，無論是傳統的 Unix 或 Windows 伺服器，皆會成為勒索軟體、內部威脅及進階持續性攻擊者建立一個擴大的攻擊面。

產業趨勢帶來全新的緊迫感

- 混合IT的現實：80% 企業表示關鍵工作負載仍分散於雲端、Unix 及傳統基礎架構。
- 勒索軟體激增：攻擊者鎖定生命週期終止與未修補系統，因防禦方可選擇的安全防禦方案有限。
- 使用生命週期被迫延長：經濟環境與整合複雜性常迫使企業將傳統系統使用期限大幅延展至原廠官方支援時限之外。
- 數位轉型壓力：企業必須在不中斷關鍵業務的前提下推動現代化--要在這兩種對立的想法之間取得微妙平衡，會是一大挑戰，其中保護傳統資產更是不可妥協的底線。

DCS：不止於為老舊作業系統打造的防禦解決方案

賽門鐵克重要主機防護系統：DCS～Data Center Security 專為保護 Unix、Linux 及傳統 Windows 系統抵禦現代威脅而設計。有別於高度依賴特徵檔或修補週期的被動式工具，DCS 提供主動式策略防護機制，強化關鍵伺服器韌性，使其能抵禦零時差攻擊、內部人員威脅及勒索軟體攻擊。

重要功能

- 強制最小權限原則：即使 root 使用者亦受限於被核准的動作，降低內部人員濫用風險並防範權限提升攻擊。
- 微分段技術：將應用程式與伺服器分組至安全容器中，阻斷橫向移動並在攻擊者擴散前隔離受感染系統。
- 系統強化與持續監控：DCS 持續監控虛擬與實體伺服器，提供即時合規性檢查並鎖定易受攻擊的設定。
- 零時差漏洞防護：透過應用程式隔離與白名單機制，DCS 可阻斷未授權程序，並在修補程式發布前即保護記憶體免受緩衝區溢位、遠端程式碼執行攻擊及應用程式漏洞侵襲。
- 入侵防護系統 (IPS) 與檔案完整性監控 (FIM)：預建的 Unix 基準政策 (Unix baseline policies) 監控特權指令、系統強化狀態、登入活動及檔案完整性，即時偵測異常行為。
- 針對 Unix 特定威脅的防禦機制：從類似 Shellshock 的 Bash 漏洞到 Linux.Gomir 後門程式，DCS 可阻止惡意程式碼執行，強制對敏感設定實施唯讀保護，並將變更行為與核准的管理流程綁定。
- 網路流量控制：精細可微調的政策可精準限制未受信任之連線、縮小攻擊面，並將通訊範圍限制於已知且經授權的系統。
- 威脅情報整合：透過整合賽門鐵克的全球威脅情報與機器學習技術，DCS 能阻擋針對 Linux／Unix 系統的新型惡意軟體家族，防止惡意程式建立持續機制及指揮與控制通訊。

成功案例

- 穩定是金融服務的基石：全球前五大銀行持續透過逾二十年歷史的 Unix 伺服器處理每日數百萬筆交易。將這些工作負載遷移至雲端不僅成本高昂，更伴隨營運風險。透過部署 DCS，該銀行達成：
  - 即時防堵未修補漏洞。
  - 資安事件應變處理時間縮短 45%。
  - 實現混合 IT 環境的持續合規性報告。
- 守護醫療基礎設施：某大型醫療機構運用 DCS 對仍運行但生命週期已終止的 Windows Server 上關鍵醫療系統實施唯讀保護。此舉在不中斷重要服務的前提下，有效阻止勒索軟體篡改病患資料，並確保符合 HIPAA 規範。

保護過去，確保未來

企業絕不能將傳統系統視為過時的遺物。它們是是活生生、會呼吸的資產--全球營運的支柱。保護這些資產不是可有可無的選項，而是面對勒索軟體、監管壓力與數位轉型時，企業韌性的核心所在。

透過 DCS 解決方案，組織能延長最值得信賴系統的安全與合規生命週期，確保舊系統不再成為負擔，而是堅不可摧的堡壘。

關於賽門鐵克的重要主機防護系統：DCS～Data Center Security 的完整資訊可點擊網頁說明或最新簡報檔。網頁或簡報如有說明不夠清楚的地方，歡迎與保安資訊的業務或技術顧問提供建議。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片）軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。