連鎖零售商確保 PCI DSS 法規遵循

大型零售商利用 Quest® 解決方案，輕鬆通過年度 PCI DSS 稽核，同時維持整個企業的高強度安全性。

「爲了 PCI DSS 法規遵循，我們必須開啓所有原生記錄，並爲稽核人員提供過去一年的完整記錄…要不是有 InTrust，我們老早就用完空間了。」

大型連鎖零售商，企業系統管理員

客戶簡介

行業 零售業

國家/地區 美國

業務需求

爲了通過年度 PCI DSS 稽核並確保安全性，一家大型連鎖零售商需要企業級的記錄管理與符合成本效益的長期資料儲存方式，同時也需要進階的 Active Directory 監控和變更稽核功能。

解決方案

有了 Quest® InTrust®，該公司現在可從其 4,000 個 POS 端點和監管之零售 IT 環境中的其他系統收集資料，並將所有資料以高度壓縮的格式保存數年，同時保留簡單、安全的存取方式以供法規遵循稽核和安全性調查所用。此外，多虧了管理責任的安全委派和物件保護等功能，Quest Change Auditor 與 Active Roles 還可爲公司的業務 IT 環境提供全面的安全防護機制。

優點

- 可有效率地收集，並以符合成本效益的方式儲存 PCI DSS 稽核所需要的所有資料。
- 藉由實現對 Active Directory 的強大控制，提升安全性。
- 確保一致性並實現管理工作的安全委派，進而節省時間。
- 防止對系統管理員帳戶和其他關鍵 AD 物件的變更，藉此封鎖攻擊。

解決方案簡介

- Microsoft 平台管理

現代化零售組織必須維持支付卡產業資料安全標準 (PCI DSS) 的法規遵循，並在年度稽核時證明其確實遵循。稽核失敗可能會導致無法接受信用卡付款，如此將危害整個企業。PCI DSS 的其中一項要求可能特別難以達成：保存過去一年的完整 IT 稽核軌跡。但有一家大型連鎖零售商藉由 Quest Software 的解決方案，從其整個零售 IT 環境收集需要的記錄資料、按照規定以符合成本效益的方式妥善保存，同時維持其業務 IT 環境的高強度安全性。

「我們在 Active Roles 中的原則可以讓 Active Directory 保持井然有序，並確保所有事情都以一致的方式執行，如此便可簡化管理員和我的工作。」

大型連鎖零售商，
企業系統管理員

PCI DSS 法規遵循對任何現代化零售企業都非常重要。

零售商必須收集其整個受監管 IT 環境的記錄資料，藉此維持 PCI DSS 法規遵循。然而，現代化 IT 生態系統往往相當忙碌，同時有各種系統收集大量的關鍵記錄資料。一間大型連鎖零售商的 IT 團隊，體認到編寫指令碼和其他人工方式，顯然不是用來通過稽核的合適作法。相反地，他們需要可從各種系統 (包括橫跨數十個遠端位置的 4,000 個銷售點 [POS] 端點) 收集所有必要資料的企業級解決方案，並將資料以符合成本效益的方式保存至少一年 (應 PCI DSS 要求)。

除了受監管的 POS 環境之外，IT 團隊也需要負責看顧所有現代化組織都會用來處理一般業務營運 (如 Exchange 及人力資源系統) 的系統。在威脅態勢演變快速的情況下，他們渴望能夠更妥善地保護其 Active Direcrtory 免於外部攻擊、惡意內部人士及系統管理員失誤或不當操作所害。爲了提供如此嚴密的安全機制，他們需要一種方法讓 AD 保持井然有序，並密切監控對 AD 物件 (包括使用者和群組) 的所有變更。

來自 ACTIVE DIRECTORY 專家的業界最佳解決方案

在仔細評估市場提供的選項後，該零售商選擇了四項 Quest 解決方案。InTrust® 是可擴充的智慧型事件記錄管理工具，可讓您監控 Windows、UNIX/Linux、資料庫、應用程式、網路裝置等等的所有使用者工作站和系統管理員活動。不只如此，其 20:1 的資料壓縮率可讓您以符合成本效益的方式，將事件記錄保存數年。InTrust 甚至可以提供即時警示搭配自動化動作，以確保對可疑活動立即做出回應。

Active Roles 可簡化使用者和群組管理工作，大幅提高安全性。您可以在單一虛擬介面中，以自動化、一致且全面的方式，輕鬆管理內部部署或混合式 AD 環境的所有系統。

產品和服務

軟體
Active Roles
Change Auditor for Active Directory
Change Auditor for Windows File Servers
InTrust

Change Auditor for Active Directory 和 Change Auditor for Windows File Servers 可追蹤、稽核、回報並通知所有的重要組態變更，甚至主動保護關鍵物件 (例如系統管理帳戶和群組) 免於遭到更改。

用 INTRUST 確保並證實 PCI DSS 法規遵循

該公司快速設定了 InTrust 以從整個受監管之零售 IT 環境的多個系統收集資料。其企業系統管理員表示：「我們每一個 POS 端點都有 InTrust，」「我們也使用 InTrust 來收集 SQL Server、終端伺服器、FTP 及 IIS 的記錄。我也會從一部伺服器擷取自訂文字記錄，我們還會收集一些系統記錄。」

這些資料都經過高度壓縮並儲存在 InTrust 中央存放庫，以符合成本效益的方式長期保存，以滿足法規遵循及安全性的需求。該系統管理員解釋道：「爲了 PCI DSS 法規遵循，我們必須開啓所有原生記錄，並爲稽核人員提供過去一年的完整記錄。」「我們有相當多的端點和活動，因此也有很多的資料，我們隨時都有大約 800 GB 的記錄量。要不是有 InTrust，我們老早就用完空間了。這對業務來說可能會是場災難：如果我們無法符合 PCI 的要求，從長遠來看，我們便無法接受信用卡付款。」

但是多虧了 InTrust 提供的進階壓縮功能，該公司不再需要擔心無法提供稽核人員所需的資料。該企業系統管理員如是說：「InTrust 的壓縮率非常高，」「它絕對爲我們節省了很多空間，讓我們能儲存 PCI DSS 法規遵循所需的所有記錄資料。事實上，要是沒有 InTrust，我甚至不認爲眞的能收集所有的資料，更別提將其保存起來，因爲要傳輸如此大量的未壓縮資料便需要大量的寬頻。」

可輕易搜尋且預先建立的報告和進階警示

再者，InTrust 可確保 IT 團隊快速存取所需的特定資料以進行安全性調查、立即回答稽核人員的問題，以及維持安全性。該系統管理員說道：「有了 InTrust 存放庫的進階索引功能，搜尋資料變得快速又輕鬆。」「隨時取用的報告幾乎涵蓋了所有我需要的內容，讓我不用去找仍未經設定的東西。」

主動式警示也對安全性和法規遵循相當重要，該公司對於 InTrust 的即時警示功能相當滿意。該系統管理員補充：「我在 InTrust 裡爲幾乎所有在 Active Directory 中處理的項目設定了警示，無論是建立新使用者或加入機器，」「這對通過稽核來說是很關鍵的。舉例來說，如果有技術人員更換了端點，該端點會重新加入，而我們便會取得該動作的警示。稽核人員會要求查看該警示，以證明我們有按照對應服務台工單的要求，確實更換端點。有了 InTrust 警示，我能取得所有需要的項目，包括稽核人員要求的所有資訊。」

以 ACTIVE ROLES 和 CHANGE AUDITOR 保護 AD 並讓其井然有序

在辦公室和倉儲業務營運 (如 Exchange 訊息) 專用的 IT 環境中，該公司仰賴 Active Roles 來維持嚴密的安全性。系統管理員說道：「我們使用 Active Roles 已經有五、六年了。」「在那之前，Active Directory 簡直是一團糟，而且每個管理員都有自己的一套做事方法。現在，大約十餘名管理員都能存取 Active Directory，而 Active Roles 則是唯一的途徑。我們在 Active Roles 中的原則可以讓 Active Directory 保持井然有序，並確保所有事情都以一致的方式執行，如此便可簡化管理員和我的工作。舉例來說，Active Roles 現在會強制管理員從一開始便以正確的 OU 建立所有電腦帳戶，因此我就不必之後再使用 PowerShell 移動帳戶。」

> 「我們請來的測試人員非常驚訝，因爲他們無法突破 Change Auditor 物件保護。」
>
> *大型連鎖零售商，企業系統管理員*

「即使我們擁有如此多的授權產品，我也很少致電給支援團隊，大概一年也只會打一次。但每當我致電時，支援團隊都能給我很大的幫助並解決我遇到的問題。」

大型連鎖零售商，
企業系統管理員

Active Roles 還能讓最高系統管理員精細委派權限給其他管理員，以利在全盤掌控的情況下分擔工作負荷。他解釋道：「Active Roles 幫我省下很多時間，這對我來說尤其重要，因爲我有許多種工作要做，且我全年無休都在待命。」「以前我只能委派工作給少數管理員，因爲我不能請服務台之類的工作人員到 Active Directory 進行變更。Active Roles 讓我可以委派更多工作，因爲我能掌控每個人的權限。舉例來說，我們在各店面都配有主管。如果其中一位要連絡服務台並請他們重設密碼，服務台無法執行此操作；只有可驗證申請者身分的區域經理可更改主管的密碼。」

兩項 Change Auditor 解決方案可爲環境增添更多安全性。Clark 說：「Change Auditor 物件保護幫了我極大的忙，」「我設定這項功能來防止檔案伺服器上特定目錄中的 ACL 遭到變更，並同時保護所有系統管理帳戶。我們請來的測試人員非常驚訝，因爲他們無法突破 Change Auditor 物件保護。」

世界級支援

其企業系統管理員對 Quest 支援服務更是讚譽有加。他說道：「即使我們擁有如此多的授權產品，我也很少致電給支援團隊，大概一年也只會打一次。」「但每當我致電時，支援團隊都能給我很大的幫助並解決我遇到的問題。Quest 社群上的支援論壇也很有幫助，關於一些我們沒有徹底利用的功能，我們獲得了很多想法和建議。」

關於 QUEST

Quest 爲快速變遷的企業 IT 世界提供軟體解決方案。我們可協助簡化資料暴增、雲端擴張、混合式資料中心、安全性威脅和法規要求所帶來的難題。我們的產品組合包含用於資料庫管理、資料保護、統一端點管理、身分識別與存取權管理，以及 Microsoft 平台管理的解決方案。

前往 Quest.com/Customer-Stories 檢視更多個案研究

CaseStudy-RetailerPCIDSS-TW-KS-zh_TW-WL-55478#