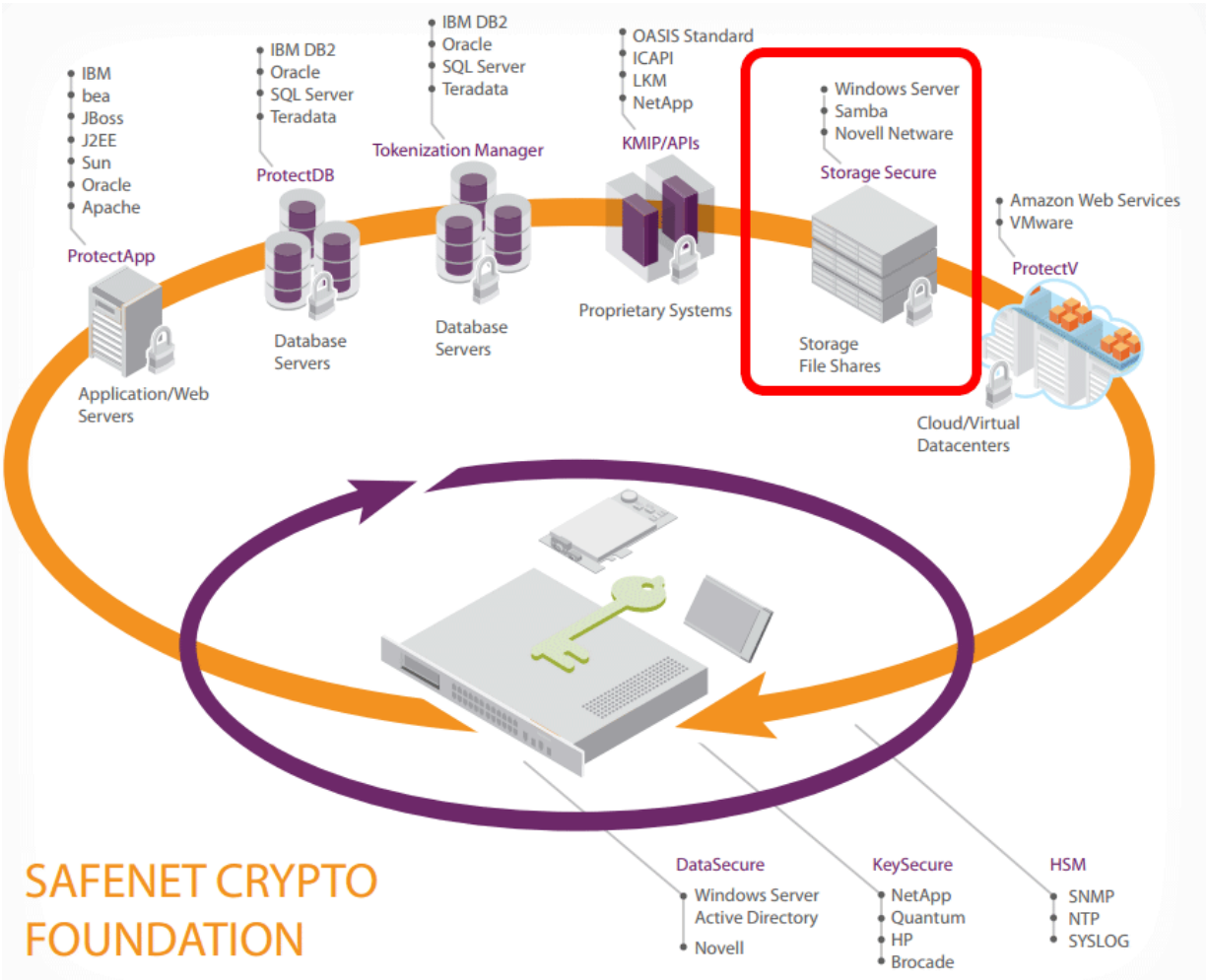
SafeNet
網路儲存加密設備 (StorageSecure) 應用案例

文章來源：SafeNet　翻譯整理：叡揚資訊 資訊安全事業處

企業資料是有價值的商品。如果它落入壞人之手，它不僅在業務上有負面影響也可能使該公司在因未能遵守資料安全法規遭受到法律責任及處罰。保護資料避免遭受未經授權的使用是任何業務上重要的考慮。有一種控制資料存取的方法是通過加密儲存在 Disk 上的資料。複製文件，沒有正確的加密 / 解密金鑰即使實際取得 Disk 也將無法獲得訪問這些資料。

SafeNet StorageSecure 加密裝置，提供安全小組有效且持續的關鍵能力，滿足其治理、法規遵從性和資料保護任務。此文件：StorageSecure; 一個獨有的的資料加密解決方案，安裝在乙太網網路，以保護如 SMB (CIFS) 和 NFS，以及 iSCSI LUN 的共用資料夾內常見的業務案例。

SafeNet 資料保護方案架構：



業務案例 1：多用戶環境保護知識產權需求

越來越多組織地採用多方租用和雲端計算環境所提供的成本效益。雖然資源分享有幾個好處，無論是在本地或在雲端中資料分離和安全成為更加至關重要的問題。您的組織可以證明在多用戶環境中充分保護知識產權未經授權的披露嗎？

解決方案： SafeNet StorageSecure 藉由現有的基礎設備提供統一的金鑰生命週期管理、資料的隔離和保護在多用戶或雲端環境的知識產權。這實現了被保護的資料免受特權管理者未經授權的存取或竊取。StorageSecure 提供單一、集中式政策執行和稽核控制橫跨實體和虛擬的資料中心、災害復原網站和雲端架構，解決您共用基礎架構環境中任何合規性的要求。

業務案例 2：滿足法規要求

組織有法律和信託責任確保企業資料符合政府法規和企業安全性原則。根據具體的法規；如 PCI DSS、HIPAA、SOX 等，敏感性資料必須妥善處理，以免組織遭遇安全漏洞和暴露本身的法律和 / 或財務負債。您的組織能夠證明其靜止的資料是完全符合監管要求？

解決方案： SafeNet StorageSecure 幫助您滿足法規要求，從而確保受保護的資料將被加密並且為未經授權的使用者無法讀取。你可以納入現有使用者的存取控制清單和身份驗證控制機制，例如 LDAP、微軟 AD 目錄、NIS 和 RADIUS。在 StorageSecure 管理主控台額外的雙重授權控制層可以進一步限制存取在陣列中的敏感性資料和並防止特權管理員。StorageSecure 基於業務政策進行進行資料加密，並確保資料隔離通過加密與單一、 集中式的政策執行和遵守稽核控制機制。只有授權的人員擁有有權訪問的加密金鑰。StorageSecure 提供了細緻化保護 SMB (CIFS) 和 NFS 檔案共用以及 iSCSI Lun，且無需中斷使用者的工作流程，讓你就可以放心的使企業資料符合法規要求。

業務案例 3：需要保護以防無意的合法洩露

Google 和微軟最近宣佈了有多少次執法部門要求訪問其在雲端礎設施上儲存的訊息。Google 不能透露確切的數位但在 2012 年估計大約有 9,000 次要求，而微軟收到 11,000 的要求。雲端服務提供者並不是一直能自由地告知正在被調查的使用者當發出了一個緘口令。在資料儲區包含多個用戶的資料時，其他用戶的資料可能被當局無意中獲得。您的組織可以證明它的資料是謹慎保護和免受無意中合法洩露嗎？

解決方案：SafeNet StorageSecure 特過提供保護，防止意外合法洩漏，使企業能夠保留其資料的控制權。和在一個前提下：是由客戶維護的 KeySecure 設備，在高強度金鑰管理系統中管理加密金鑰，加密所有儲存設備上的資料。因為 KeySecure 的權責分離您組織的資料在沒有得到金鑰前不可能被存取，您在雲端環境下部署 KeySecure 保護您的資料以確保只有授權的人員將有機會獲得加密金鑰。這可以確保你知道任何嘗試訪問受保護資料的訊息。