THALES

www.thales-esecurity.com

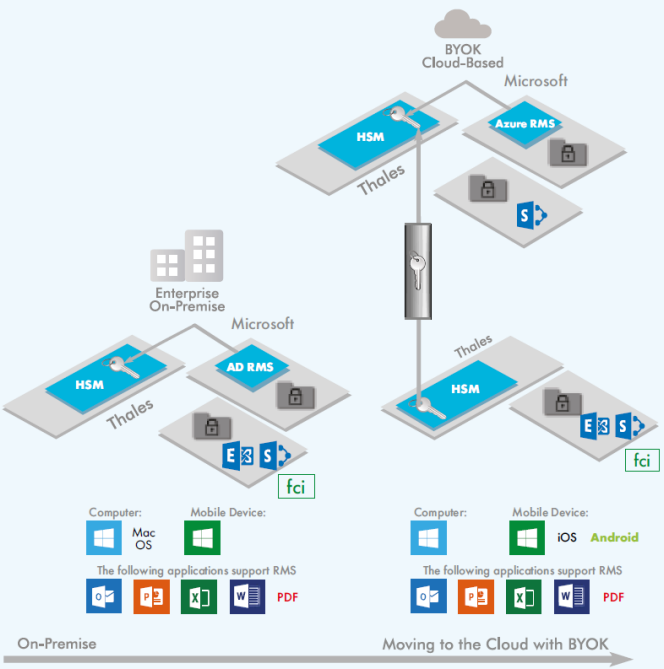
MICROSOFT 攜手 THALES，提供不間斷的資訊保護 以獨特"BYOK"選項功能，讓您充分掌握雲端資料

- 針對交換的資料執行存取即使用控制
- 提供 Microsoft RMS 佈署所需的強化金鑰保護
- 提供 FIPS 140-2 認證的金鑰生命週期管理
- 可充分控管保護機敏資料的金鑰
- 確保金鑰在 Microsoft 雲端服務裡是不可見的

Microsoft

< Thales e-security >

強化資訊安全：THALES 為 MICROSOFT RMS 所提供的高效保障解決方案



無論是在用戶端、混合式配置或是全雲端環境使用 RMS，Thales nShield HSM 都能提供關鍵金鑰不可或缺的管控。

Microsoft Rights Management Services（RMS）藉由在數位資產上嵌入可執行的安全政策保護協作環境中交換的資料，無論資料是哪種型態。RMS 為受託管的訂用服務，因此可以在沒有IT基礎架構的情況下執行所需的應用程式，並確保資訊在組織範圍內都能受到保護。

問題：協作環境需要不間斷的資訊保護

RMS 透過加密技術提供資料所需的存取控制和持續性保護，因此 RMS 安全與否，取決於關鍵加密金鑰的保護等級，暴露金鑰如同讓機敏資料暴露在風險之中。

挑戰：維持對機敏資料伺服器金鑰的管控

用硬體加密模組（HSM）部署用戶端的 AD RMS，可以防護並管理保護資料的伺服器金鑰。使用 Windows Azure RMS，不用捨棄對雲端資料金鑰的管控，Azure RMS 使用 Thales HSM，因此金鑰能一直在自己管控之下，且絕不會被 Microsoft 看到。

強化資訊安全：THALES 為 MICROSOFT RMS 所提供的高效保障解決方案

Thales nShield HSM 創造一個保護 RMS 訂戶金鑰的加密空間，能消除雲端機敏資料充滿弱點的疑慮－因為安全基礎架構被共享，所以雲端只能當成一種共享服務。

解決方案：Micorsoft RMS 結合 Thales，強化金鑰管控

Thales nShield HSM 在用戶端和雲端的 Microsoft RMS 部署中，對伺服器金鑰的使用及管利提供嚴格的管控。

- **使用用戶端** AD RMS：Thales nShield HSM 提供保護關鍵伺服器金鑰的硬體解決方案， 可獨立於軟體環境外，管理防護伺服器金鑰。
- **訂用** Azure RMS：伺服器金鑰即為訂戶金鑰。在預設情況下，Azure RMS 會生成、管理訂戶金鑰的生命週期，但您可以選擇用 Thales HSM 保護訂戶金鑰。Thales HSM 能生成、管理、防護訂戶金鑰，讓您而非 Microsoft 管控金鑰。
- **選用** BYOK：Thales 提供基於雲端環境的獨特功能，可依企業IT政策在用戶端生成訂戶金鑰，並安全地傳輸到由 Microsoft 託管的 Thales nShield HSM，進而有效滿足用戶端 RMS 部署的安全準則。
  雖然 Azure RMS 可以使用訂戶金鑰並將其複製用於毀損回復，但 Microsoft 無法查看或存取訂戶金鑰。BYOK 可確保訂戶金鑰不會從 Microsoft 持有的 HSM 裡回復。
  其他防護還包括近實時的使用 log 記錄，讓您可以明確知道金鑰"何時"並"如何"被 Azure RMS 使用。

為何要用 Thales HSM 搭配 Microsoft RMS？

若您現在使用的是用戶端 AD RMS 並希望保留移轉到 Azure RMS 的選項，Thales nShield HSM 可協助您輕鬆將用戶端 AD RMS 伺服器金鑰安全地移轉到 Azure RMS 訂戶金鑰環境。

Thales nShield HSM 具備以下功能，讓企業可以維持對金鑰的監管及其使用上的可視性：

- 在強化、防竄改的環境下保護金鑰
- 在 Microsoft 持有時保護訂戶金鑰
- 能讓金鑰只在 HSM 內儲存使用，訂戶金鑰可以安全地從用戶端的 HSM 傳輸到 Microsoft 的 HSM，不脫離 HSM 的防護
- 以 FIPS 140-2 認證的硬體保護訂戶金鑰，並能執行安全政策，透過存取管控機制有效執行職責分離，確保金鑰只用在獲得授權的用途上
- 透過金鑰管理、儲存及備援功能確保訂戶金鑰的可用性
- 符合公部門、金融產業和一般企業的合規要求

Thales nShield HSM 還能滿足特定效能及預算需求：

針對 high-volume 的用戶端金鑰生成和管理（或混合部署的一部分），可用 nShield Solo / Solo + / Solo XC 嵌入 PCIe 卡和 nShield Connect / Connect + / Connect XC 等網路連結設備提供高效能的硬體防護。

對 low-volume 而言，用戶端金鑰生成則是 BYOK 的部分功能，可用 nShield Edge 提供便捷的 USB 硬體防護。

Microsoft：

Microsoft 改變了企業創造、分享內容的方式，並建立了協作流程。以 Microsoft RMS 解決方案為基礎的系統都大幅提升了生產力。在保護資料上，Microsoft RMS 以加密來建立可信任的企業環境：

- 管理組織內的個別身分
- 依授權原則提供認證
- 管控使用者存取資料的權限
- 提供全面性的資料保護

Gold Microsoft Partner Microsoft

CipherTech TRUST&SECURITY 台灣區代理商
亞利安科技股份有限公司
了解更多資訊請洽 02-27992800
或至官網 http://www.ciphertech.com.tw