cpl.thalesgroup.com

THALES
Building a future we can all trust

佈局全球的汽車製造商，強化跨雲端與傳統系統整合的安全性和法規遵循

這家總部位於歐洲的大型汽車製造商，經由多年的併購和企業營運的快速擴張，在全球多個國家拓展設立製造和銷售業務。 為了支援全球性的營運，企業加快邁向數位化轉型，採用雲端和其他平台。 這也導致企業數十萬員工在全球多個本地端和雲端環境，存取大量的機敏資料。

面對日益複雜且風險逐日攀升的網絡安全環境，這家全球性企業希望主動改善總公司和各地區子公司，同時使用多個平台時對機敏資料的管控。 該企業還希望保持所有關鍵資料保護和隱私法規的遵循，不論在那個國家區域都能通過安全和合規的審查。

挑戰

該公司執行多項計劃，企業期望在混合 IT 環境中，強化機敏資料和應用程式的安全性。 計畫關注的重點項目包括：

- 保護總公司與全球子公司使用中的多個類型 Salesforce 和 Office 365 的應用程式內機敏資料。
- 確保儲存在多個傳統系統，包括 Windows、Linux 和 Hewlett Packard UX 上的機敏資料的合規性，來保障資料隱私與安全的合規要求。
- 對公司在各國家/區域內的數十萬名員工，執行更高階的內部機敏資料的存取控制與管理

解決方案

在多個推動流程中，Thales 協助該企業保護多個本地端和雲端系統中的機敏資料，並管控總部和子公司成千上萬名員工的存取權限。

Thales 經由使用 Ciphertrust Cloud Key Manager (CCKM) 解決方案的集中式金鑰管理生命週期，簡化了對 Salesforce 和 Office 365等雲端軟體即服務平台上的資料保護。 CCKM 解決方案透過單一管理平台、自動化金鑰生命週期管理，實現對跨平台和多租戶的加密金鑰的完全控管，並在雲端服務供應商自帶金鑰 (BYOK) 服務和汽車製造商安全團隊之間，實現強大的職責分離。

採用 Thales Ciphertrust Transparent Encryption 集中式金鑰管理，保護儲存在多個傳統系統，包括 Windows、Linux 和 HP UX 上的機敏資料的安全，保障資料隱私與安全的合規要求。Ciphertrust Transparent Encryption 協助汽車製造商對機敏資料進行加密、定義存取安全並執行細粒度的安全策略，有效降低外部攻擊和特權憑證被濫用的威脅。

最後，Thales 經由 Luna Luna Hardware Security Modules(HSM) 信任根，實施以 PKI 為基礎的存取管理和身份認證，確保全球數十萬名員工從多個國家/區域能安全地存取機敏資料和應用程式。

成果

這家全球性的汽車製造商能夠提供高安全性，降低整個企業的資料外洩風險，並提高整體合規性要求。 集中式金鑰管理有效提高雲端軟體即服務環境的安全性，同時確保子公司員工們繼續使用雲端服務的便利，也保障機敏客戶和企業資料的高安全性。

集中執行適用於傳統環境的資料細粒度安全策略，增強公司的整體安全維護，並加快對全球支付卡產業資料安全標準(PCI)和歐盟通用資料保護條例 (GDPR) 立法等法規的遵循。 強大的基於 PKI 的存取管理和身份認證，使數十萬名員工能夠存取內部機敏的資源，而不會在每次存取時發生資料外洩的風險。

關於Thales

任何企業都信賴 Thales 來保護他們資料的隱私權。在資料安全方面，企業面臨著越來越多的決定性時刻。無論是建置加密策略，移轉到雲端還是滿足合規性要求，在邁向數位化轉型時，您可以信賴 Thales 來保護您的有價資料。

關鍵時刻 關鍵技術

挑戰

- 在 Salesforce 和 Office 366 中保護機敏資料
- 改善隱私和資料在合規性的安全現況
- 對機敏資源執行更安全的存取控制

解決方案

- Ciphertrust Cloud Key Manager (CCKM)
- Ciphertrust Transparent Encryption
- Luna Hardware Security Module

成果

- 以集中式金鑰管理提高雲端 SaaS 環境的安全性
- 透過集中化執行細粒度安全策略，，加速達到合規性
- 透過基於 PKI 的存取管理，確保數十萬員工的安全存取

> cpl.thalesgroup.com <

聯繫我們 – 有關全球辦公室地點與聯繫資訊，請參訪 cpl.thalesgroup.com/contact-us