cpl.thalesgroup.com

THALES

Thales Data Protection on Demand

不只是資料保護
是隨選即用的資料保護

Thales Data Protection On Demand 雲端平台透過簡易的線上市集，提供各式雲端硬體安全模組（HSM）和金鑰管理服務。有了 Thales Data Protection On Demand（DPoD），不必再購買、部署或維護任何硬體，讓資安管理變得更加簡易、符合成本效益且便利。只需幾個按鍵，便能在幾分鐘內部署所需的保護措施、提供服務、新增資安政策並且查看使用狀況報告。

選擇適合您的資安保護方案 – 只需幾分鐘的時間

有了 Thales Data Protection On Demand，您只需輕鬆點擊便可取得各種資安服務，並且部署您所需的服務，以保護各式應用程式及使用案例。就是這麼簡單。

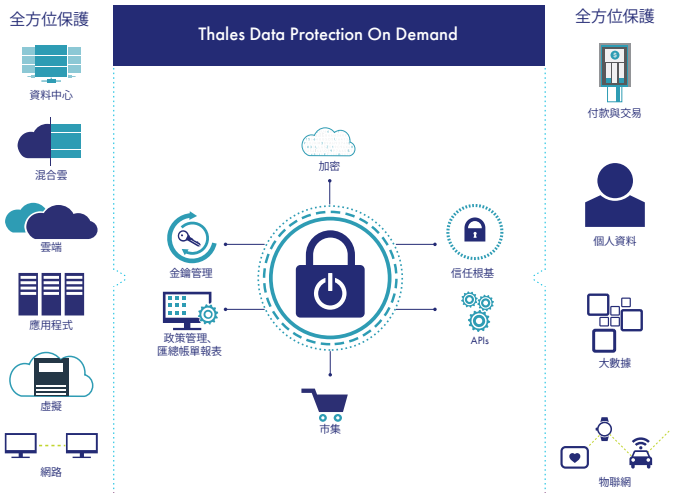
零預付款，用多少付多少

無需購買軟硬體、支援或更新方案，無任何資本支出。此外，獨特的付費方式，用多少付多少，可視需求彈性購買服務，滿足貴企業多變的業務需求。

隨時隨地保護資料並達到合規標準

有了 Thales Data Protection On Demand，您能夠在任何環境（雲端、虛擬或企業內部）保護敏感資料，以便管理您的資安政策，並且符合法規和合規要求。保護您所建立、儲存及分析的資料。加密您的應用程式：區塊鏈、雲端和物聯網。

保護資料，隨選即用



集中控管所有雲端金鑰

不論您使用的是 Salesforce.com、Amazon Web Services、Google、IBM 或 Microsoft Azure，或者是合併使用雲端及內部解決方案，您都能隨時控管金鑰。

輕鬆與您的雲端和 IT 服務整合

Data Protection on Demand已提供預先組態的APIs，讓你能夠輕易的整合Luna Cloud HSM與CipherTrust Cloud Key Management服務以保護你的應用程式和資料。Thales藉由支援third party HSM整合、共同SDK與API支援、以及地端Luna設備與DPoD服務的高可用性群組存取，在Luna Cloud HSM服務與地端Luna HSM appliances之間提供無縫隙的金鑰轉移，協助客戶確保他們的資料和加密金鑰的安全，而不論資料駐留在何處。

強大的可擴充性及靈活彈性

可依您的需求變更，自動調整HSM和金鑰管理服務的規模。輕鬆無限制地增加HSM和金鑰管理服務的容量和加密資源。

讓您專注於業務營運，不必再為管理資安軟硬體操心

使用Thales Data Protection On Demand時，您無須針對您的 HSM、金鑰管理或加密需求另行購買、供應、設定或維護硬軟體。所有的軟硬體和基礎結構皆由 Thales負責管理並且隨附服務等級協定（SLA），您只需專注於業務營運即可。

託管服務供應商適用的隨選資料保護

我們的供應方式讓 Thales 合作夥伴能夠為其客戶提供強大的資料保護服務，同時讓他們能夠使用自有品牌，與其他既有的雲端服務商品一同搭售。有了Thales Data Protection On Demand，服務供應商能輕鬆快速地為其客戶提供數十年來經業界實證的金鑰管理和加密服務。

- 零預付款項
- 雲端價格–僅基於營運支出的使用計費
- 隨選即用
- 支援多租用戶，能夠完全分割／分離不同客戶的金鑰
- 集中化管理
- 包括自動備份和故障轉移

立即行動

雲端安全應用程式不斷推陳出新，數百個適用業界標準PKCS11介面的應用程式讓您隨手可得，您可以在眾多選項與整合方案中挑選您所需要的資安服務。

Luna雲端硬體安全模組服務

- **HSM on Demand** – 設定並存取 Cloud HSM 服務作為貴企業加密作業的信任根基
- **HSM on Demand for CyberArk** – 確保CyberArk特權存取解決方案中的top-level加密金鑰在HSM中的安全性
- **HSM on Demand 數位簽章** – 對軟體和韌體套裝軟體或電子文件進行數位簽章，以確保發送方的完整性
- **HSM on Demand for Hyperledger** – 為區塊鏈交易提供信任機制，以便在分散式系統中執行所需的加密作業
- **HSM on Demand for Java Code Signer** – 使用HSM產生的加密金鑰，在Java物件上進行加密簽署作業
- **HSM on Demand for Microsoft 目錄服務** – 確保Microsoft Root CA金鑰在HSM中的安全性
- **HSM on Demand for Microsoft Authenticode** – 在HSM上產生並確保Microsoft Authenticode憑證的安全性
- **HSM on Demand for Microsoft SQL Server** – 卸載Microsoft SQL Server對HSM的加密作業
- **HSM on Demand for Oracle TDE** – 確保原生的Oracle TDE加密功能所使用的資料金鑰可透過HSM內儲存的主要金鑰進行加密
- **HSM on Demand for PKI Private Key Protection**– 確保負責建立PKI信任階層的憑證授權單位所屬私有金鑰的安全性
- **Luna Backup HSM** – 為企業內部部署的Luna HSM進行備份和還原

CipherTrust Cloud金鑰管理服務

- **Key Broker for Azure**–安全地生成加密密鑰並將其導入到Azure Key Vault中，從而為Microsoft基礎結構啟用BYOK
- **Key Broker for Salesforce** - 建立Salesforce的金鑰組成因素（用戶密碼），並且管理貴企業的金鑰和資安政策，以便在其生命週期內與Salesforce Shield達成一致

合作夥伴服務

Data Protection on Demand（DPoD）已將其服務能力擴展到包括合作夥伴主導的安全服務，從而擴展了Thales Luna HSMs在整個安全生態系統中廣泛集成的價值。

Thales的優勢

Thales作為雲/環境不可知的資料保護市場領先者，經過30多年的驗證和認證，是唯一一家提供廣泛HSM部署選項的供應商，它提供了一種真正的混合HSM，可以在本地和基於雲的環境之間分配工作負載，並保持組織加密對象基於雲的備份的實時性。Thales還為越來越多的CSP和SaaS提供商提供了多種自帶金鑰（BYOK）解決方案，包括密碼信任雲金鑰管理服務，由DPoD提供支援。

技術規格

支援應用程式編程介面

- PKCS#11、Java 和 OpenSSL，Linux 用
- PKCS#11、Java 和 CSP/KSP，Windows 用

加密

- 完整支援 Suite B
- 非對稱或演算法：RSA、DSA、Diffie-Hellman、Elliptic Curve加密演算法（ECDSA、ECDH、Ed25519、ECIES），搭配命名、使用者自訂和 Brainpool 曲線、KCDSA
- 對稱式演算法：AES、AES-GCM、Triple DES、DES、ARIA、SEED、RC2、RC4、RC5、CAST
- 雜湊／訊息摘要／HMAC：SHA-1、SHA-2、SM3
- Key Derivation：SP800-108 計數器模式
- Key Wrapping：SP800-38F
- 隨機數產生：FIPS 140-2 認證 DRBG（SP 800-90 CTR 模式），符合 BSI DRG.4

服務效能

- 標準服務；最高可達 100 次／秒
- 最高可儲存 50 組非對稱金鑰；及／或 100 組單一服務對稱金鑰
- 單一服務最多 5 個用戶端應用程式

安全認證

- FIPS 140-2 Level 3
- ISO 9001、14001、27001、27015（銀行）、27018（GDPR）

關於 Thales

不論任何企業在個資保護的技術上都透過Thales保護他們的資料。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，您可以依靠Thales來保護您的有價資料。

關鍵時刻，關鍵技術

與我們聯繫： Dpodondemand@thalesgroup.com

註冊一個DPoD的30天試用版