cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform
發現、保護和控制

IT 團隊需要一個以資料為中心的解決方案，以確保資料從網路遷移到應用程式和雲端時的安全。 當邊界網路控制與端點安全措施失效時，以資料為中心的解決方案，使企業能夠始終符合不斷變化的隱私法規，並支援為數眾多的遠距工作員工需求。

CipherTrust Data Security Platform (CDSP) 是以資料為中心的解決方案，可顯著降低整個業務的風險，無需龐大資源即可維護強大資料安全。

CDSP 透過集中式金鑰管理，整合資料發現和分類、資料保護和細緻化存取控制。 藉由集中和簡化資料安全，CDSP 加快了法規遵循並確保雲端移轉的安全。

關鍵功能

- 集中化管理控制台
- 監督與報告
- 資料發現與分類
  - 風險分析與資料視覺化
- 資料發現和分類可結合透明加密，自動在文件級別加密機敏資料
- 勒索軟體防護
  - 主動監控惡意行為
  - 透過行為監控和資料分析，能夠達成以下功能：
    - 防範零時差攻擊
    - 當系統無法連上網路時，亦可提供保護
    - 在端點有勒索軟體潛伏時，安裝後提供保護
- 機密管理
  - 集中管理各類的機密(密碼)
  - 專為 DevOps 簡單使用而建構的整合、自動化和協調
  - 無論員工或機器存取檔案，都能在混合、多雲（所有雲端）、多租戶、本地和傳統系統環境中，完善管理機密(密碼)
- 資料保護技術
  - 檔案、資料庫與大數據的透明加密
  - 應用程式層級資料保護
  - 格式保留加密(FPE)

- 代碼化(Tokenization)與動態資料遮罩
- 靜態資料遮罩
- 特權使用者存取控制

- 集中化企業金鑰管理
  - 遵循FIPS 140-2的企業金鑰管理
  - 廣泛的KMIP整合夥伴生態系統
  - 多雲平台金鑰管理
  - 資料庫加密金鑰管理(Oracle TDE, big data, MS SQL, SQL Server Always Encrypted, etc.)

法規遵循

CipherTrust Data Security Platform 支援全球安全和隱私法，包括：支援全球安全和隱私法，包括：

- GDPR
- PCI DSS
- HIPAA
- SOX/GLBA
- CCPA
- FIPS140-2
- FISMA, FedRAMP
- NIST 800-53 rev.4
- 南非POPI Act
- ISO/IEC 27002:2013
- 日本My Number Compliance
- 南韓 PIPA
- 印度Aadhaar Act
- 菲律賓Data Privacy Act
- Monetary Act of Singapore
- 澳洲 Privacy Amendment

關鍵效益

- **簡化資料安全性。**透過次世代統一資料保護方案，發現、保護和管控任何地方的機敏資料。CipherTrust Data Security Platform（CDSP）藉由一個集中化管理控制台以簡化資料安全管理，為企業提供強大的工具以協助發現和分類機敏資料、對抗外部威脅、防範內部濫用、以及建立持續的控制，即使是資料儲存在雲端或任何外部服務供應商的基礎設施中，也能對內部和基於雲端的資料進行管理。企業可以輕鬆發現和縮小隱私漏洞、檢測和阻止勒索軟體、管理機密、確定保護的優先順序，從根本上改變企業的運營方式，事先在實施數位轉型和為客戶提供價值前，就擬定正確的隱私與安全決策。
- **加速法規遵循時程。**執法與稽核人員要求企業必須管控那些受管制和機敏的資料，並提出報告佐證。CipherTrust Data Security Platform的功能，例如資料發現與分類、加密、存取控制、稽核日誌、代碼化以及金鑰管理等，能支援無所不在的資料安全性和隱私要求。 這些管控可以快速增加到新部署，或因應演變中的法規需求而建置。 集中化且可延伸的平台功能，讓企業可以透過增加授權快速增加新控制，以及因應新保護需求而部署所需的連接器。
- **安全的雲端轉移。** CipherTrust Data Security Platform 提供進階加密與集中化金鑰管理方案，讓企業能夠安全的將機敏資料儲存在雲端。 該平台提供進階多重雲端攜帶自帶加密 (Bring Your Own Encryption; BYOE) 方案，以避免被雲端廠商的加密方案套牢，並藉由集中化的獨立加密金鑰管理功能，有效地保護跨多個雲端供應商的資料。無法執行 BYOE 的企業仍可以從外部透過 CipherTrust Cloud Key Manager (CCKM) 管理金鑰，以遵循業界最佳實務規範。 CCKM 支援自帶金鑰 (Bring Your Own Key; BYOK) 和保留公開金鑰 (HYOK) 用例，並簡化跨多個雲端基礎設施和 SaaS 應用程式的本地金鑰管理。由 Akeyless Vault 提供支援的 CipherTrust Secrets Management，提供企業級機密生命週期管理，包括創建、儲存、輪換和刪除所有類型機密的自動流程。

CipherTrust Data Security Platform

CDSP 由 CipherTrust Manager (CM) 和一組連接器組成。

CM 可以部署在本地端、雲端或混合雲環境中，也可以訂閱服務。

CipherTrust Manager

作為 CDSP 的管理核心，CM 簡化金鑰生命週期管理。包括金鑰產生、備份和還原，停用和刪除等活動，並支援各種使用案例（例如資料發現、靜態資料加密、企業金鑰管理和雲端金鑰管理）。CM 提供基於角色的金鑰及存取控管、強大的稽核和報告，並提供 REST API 方便企業開發及易於管理。 CM 有硬體和虛擬兩種版本。 硬體和虛擬設備可以利用嵌入式 Luna Network HSM 或選擇雲端 HSM 來啟用 FIPS 140-2 Level 3 最高級別信任根。

CipherTrust Data Discovery and Classification

CipherTrust Data Discovery and Classification找出雲端、大數據和傳統資料儲存的機敏資料，包括結構化與非結構化。 單一管理平台能輕易掌握敏感資料及其風險，對於安全漏洞、法規遵循與修復優先性等能夠做出更好的決策。 該方案提供流暢的工作流程，從政策組態、發現、分類到風險分析與報告，協助排除安全盲點與複雜性。

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption (CTE)提供靜態資料加密、特權使用者存取控制和詳細的資料存取稽核日誌。 代理程式保護Windows、AIX和Linux OS檔案、儲存卷與資料庫的資料，涵蓋雲端與大數據環境的實體與虛擬伺服器。 CTE的Live Data Transformation延伸功能提供免中斷服務的加密與資料加密金鑰更換。 再者，安全情資日誌與報告簡化法規遵循報表製程，並利用領先的安全資訊與事件管理(security information and event management; SIEM)系統加速威脅偵測。

CipherTrust Ransomware Protection

CipherTrust Transparent Encryption Ransomware Protection (CTE- RWP) 監控行為、可疑活動，並在檢測到勒索軟體跡象時阻止存取。 CTE-RWP 使用行為監控和資料分析，取代惡意軟體特徵資料庫，即使在與網路中斷連接的情況，也能保護系統免受零時差攻擊， 非常易於部署和管理。

CipherTrust Secrets Management powered by Akeyless Vault

CipherTrust Secrets Management (CSM) 是最先進的企業級機密管理解決方案，由 Akeyless Vault 平台提供支援。 CSM 保護並自動存取DevOps 和雲端工作負載中包括憑證、證書、API 金鑰和載具的機密管理。 DevSecOps 可以快速、輕鬆地將機密管理整合到多雲應用程式中，確保並加速整合和持續的交付流程。 非常易於部署和管理。

CipherTrust Intelligent Protection

CipherTrust Intelligent Protection 協助企業能夠根據機敏度、脆弱性和風險狀況快速發現，進行資料分類，並使用加密和存取控制，主動保護有風險的資料。 它整合 CipherTrust Data Discovery and Classification與 CipherTrust Transparent Encryption，以提高營運效率、加快合規時間並主動彌補安全漏洞。

CipherTrust Application Data Protection

CipherTrust Application Data Protection (CADP) 透過API提供加密功能例如金鑰管理、簽章、雜湊與加密服務，讓開發者能夠輕易確保應用伺服器或大數據節點的資料安全。 方案配備範例程式碼，讓開發者能快速確保他們應用程式處理的資料安全。 CADP 加速客製化資料安全方案開發，同時讓開發者得以免除複雜的金鑰管理責任。 再者，CADP 透過金鑰管理政策施行權責分離，僅由安全營運人員負責管理。

CipherTrust Tokenization

CipherTrust Tokenization提供Vault和Vaultless版本，協助降低資料法規(例如PCI-DSS)遵循所需的成本與複雜性。 代碼化(Tokenization)以一個代表性的代碼取代機敏資料，確保機敏資料安全且不會讓資料庫和非授權使用者與系統看到。 Vaultless版本包括以政策為基礎的動態資料遮罩。 這二種版本讓代碼化很容易與應用程式整合。

CipherTrust Database Protection

CipherTrust Database Protection方案為資料庫機敏欄位的資料加密整合了安全的集中化金鑰管理，而無需變更資料庫應用程式。CipherTrust Database Protection方案支援Oracle、Microsoft SQL Server、 IBM DB2與Teradata資料庫。

CipherTrust Key Management

CipherTrust Key Management 提供以標準為基礎的強大加密金鑰管理方案。 它簡化管理者的加密金鑰管理挑戰，確保金鑰安全並且僅配置給獲得授權者的加密服務。 CipherTrust Key Management支援多種使用例，包括：

- **CipherTrust Cloud Key Management (CCKM)** 簡化"攜帶 自有金鑰" (BYOK)、 “掌握自有金鑰” (HYOK) 和本地端金鑰管理，支援 Amazon Web Services (AWS)、Google Cloud Platform (GCP)、Microsoft Azure[1]、Oracle Cloud Infrastructure (OCI)[1]、Salesforce 和 SAP[1]。即使所有雲端金鑰都是本地端金鑰，CCKM 透過減少操作負擔來提高效率 。為客戶提供生命週期控制、雲端內部和雲端之間的集中管理，以及雲端加密金鑰的可視性，降低金鑰管理複雜性和營運成本。
- **CipherTrust TDE Key Management** 支援廣泛資料庫例如Oracle、Microsoft SQL和Microsoft Always Encrypted。
- **CipherTrust KMIP Server**集中化管理KMIP client，例如全硬碟加密(full disk encryption; FDE)、大數據、IBM DB2、磁帶歸檔、VMware vSphere和vSAN加密。

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

1 了解掌握自有金鑰 (HYOK) 對各雲端的正確支援日期，請與我們聯繫。

> cpl.thalesgroup.com <

聯絡我們 – 所有辦公室地點與聯絡資訊請參訪 cpl.thalesgroup.com/contact-us