cpl.thalesgroup.com

AKEYLESS | THALES
Building a future we can all trust

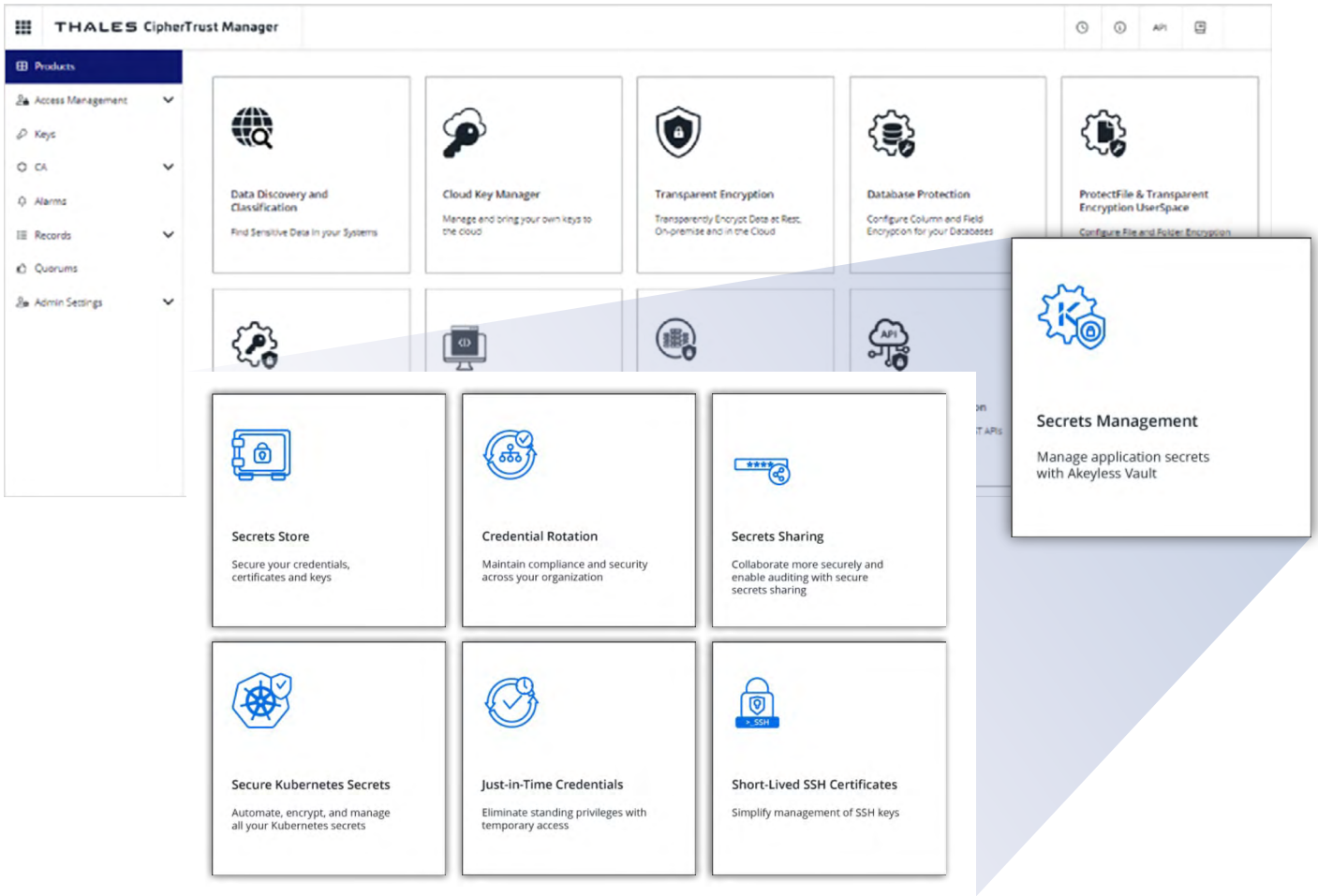
CipherTrust Secrets Management
大規模安全保護機密

CipherTrust Secrets Management（CSM）是一款由Akeyless Vault 平台支援的頂尖機密管理解決方案，可保護並自動化存取跨DevOps 工具和雲端工作負載中的重要機密資料。它包括密鑰、認證密碼、憑證、API 密鑰和權杖。這些新功能強化 CipherTrust Data Security Platform 的功能，透過優化整個營運的安全流程以降低風險。

Enterprise-ready 機密管理提供建立、儲存、輪替和刪除機密的自動化流程。透過以下功能，在您的企業中減少人為錯誤的可能性並持續執行一致的安全策略：

- 集中管理所有類型的機密性資訊
- 對 DevSecOps 提供易於使用的自動化功能
- 在混合和多雲環境中提供可擴展的 SaaS（軟體即服務）服務

單一工作流程中實現資料保護與機密管理機制



適用於所有機密資訊類型的安全儲存庫

CSM 由 Akeyless Vault 提供支援，對認證密碼、憑證和金鑰進行全面的機密管理。包括靜態機密、動態機密、SSH金鑰、API 金鑰和權杖。最重要的使用案例包括：

- 機密儲存庫
- 自動認證輪替
- 機密分享
- 動態、即時的機密生成與管理
- 機密日誌提供稽核和合規性的需求

單一工具實現金鑰管理和機密管理

結合機密管理與金鑰管理的功能，在單一位置擁有一個堅固的儲存庫，可以存放您的所有貴重資產。 透過一個服務供應商即可滿足所有資料保護的需求，實現高效運作。 CipherTrust Data Protection Platform 對資料保護的廣度和深度技術，是其他服務商無法追趕的。 藉助單一平台，無需單獨登錄，您可以經由安全閘道無縫移轉到 Akeyless Vault 平台。

減少操作的複雜性

現今有 62% 的企業並不知道它們公司內部有多少金鑰或憑證。這使得它們容易受到未經授權的存取和破壞。隨著 DevSecOps 使用越來越多的服務和工具來建構解決方案，它們依賴於金鑰和機密來對這些工具和服務進行驗證，以及與雲端的關聯驗證。因此，機密的氾濫成為加速成長的風險。隨著企業使用的服務和工具數量呈現急速增長，機密散亂使得惡意攻擊者更容易存取和破壞您的機密，這又帶來更大的災難。

透過全面分工來提升 DevSecOps 效率

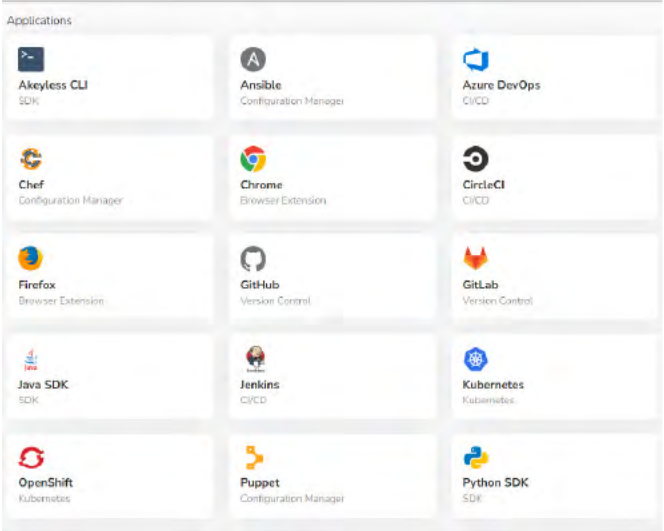
DevSecOps 可以在多雲應用程式中，快速整合金鑰管理、加密操作和機密管理，以保護並加速持續整合與交付流程。 在 DevSecOps 環境中，完全的職責分離包括將金鑰管理、加密操作和機密管理相關的責任分配給各個團隊或個人。完全的職責分離有助於防止安全漏洞，促進責任制，並改善開發、安全和運營流程的整體效率

混合式、多雲解決方案

遷移到雲端是一個過渡期，往往會形成一個混合多雲的環境，其中一些資源部署在內部，而其他資源分佈在多個公有雲和私有雲中。CSM（Cloud Service Management）主要是跨越多雲環境執行配置的工作。

無縫整合

CSM由 Akeyless Vault 提供支援，簡易的與其他第三方應用程式如 GitHub、Kubernetes、OpenShift 等整合。



快速部署和擴展

CipherTrust Secrets Management 可以從 CipherTrust Manager 儀表板中輕鬆地存取。透過使用存取 CipherTrust Manager所使用的相同認證密碼，可以從 CipherTrust Manager 儀表板中存取 CSM。這使得開始使用 CSM 變得快速而輕鬆。只需點擊 "Secrets Management" 標籤，選擇您要使用的配置，您就可以完全掌控您的機密了！

關於 Akeyless

Akeyless 獨特將創新技術和雲原生架構結合，使企業能夠快速保護 DevOps、雲端工作負載和傳統環境的安全，同時滿足合規性和法規遵循。

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