cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Transparent Encryption for Kubernetes

挑戰：保護 Kubernetes 環境的應用程式安全

容器是為服務架構套件配置和軟體相依性的必要元素。Kubernetes 是用於部署和管理這些容器的開源軟體。 使用 Kubernetes 可以更快地交付、部署和管理容器化應用程式，透過可重複使用的模組化元件提高效率、優化資源利用和降低授權費用以節省成本。 然而還是存在各種風險：

- **特權用戶濫用** – 按照預設值，Docker 依據 root 特權存取權限執行，管理員對所有租戶金鑰 (tenant secrets) 具有完全的存取權。這個不受約束的存取層級引發多種風險。如果管理員能夠不受限制的存取容器映像和其中儲存的資料，則企業可能遭受針對特權層級的攻擊。
- **跨容器存取** – 不當的權限配置可能造成多個容器存取應該保持隱私的機敏資料。此外，當容器被託管在共享的虛擬化或雲端環境中，關鍵資訊可能會暴露給第三方。
- **合規風險** – 許多合規性要求有嚴格的存取控制與稽查規範。然而，許多資安團隊在管理和追蹤容器與映像內留存資料，控制權受到限制。因此，這些資安團隊發現很難遵守相關的資安政策與法規命令。

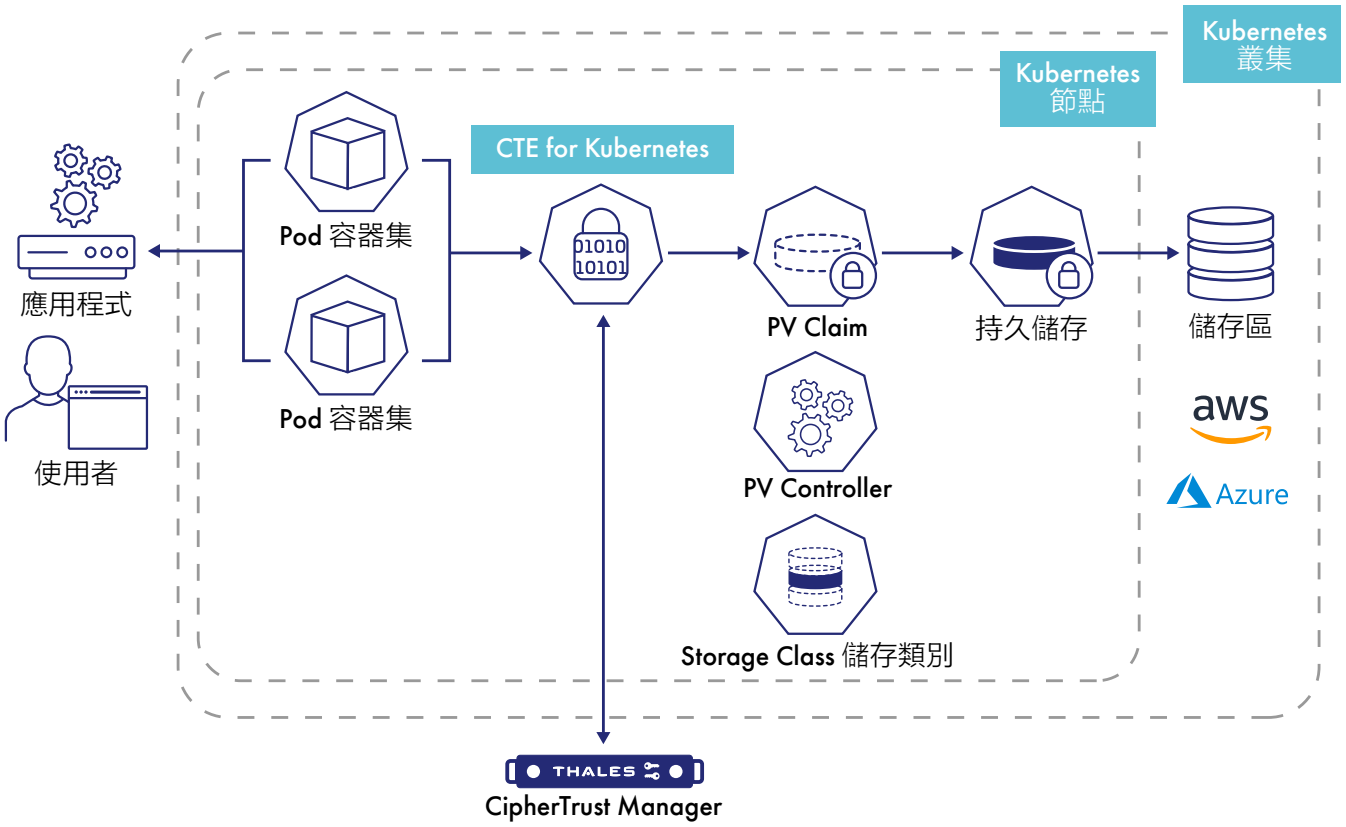
解決方案：CipherTrust Transparent Encryption for Kubernetes

CipherTrust Transparent Encryption for Kubernetes 提供用於加密、存取控制和資料存取日誌記錄的容器內核功能，使企業能夠對Kubernetes 環境中的資料建立堅實穩固的防護。 透過 CipherTrust Transparent Encrypton 的擴展，資料保護可以在每個容器的基礎上應用，兼具保護容器的內部資料，以及經過容器存取的外部儲存資料，都統一經由 CipherTrust Manager 集中管理。

優勢

CipherTrust Transparent Encryption for Kubernetes 效益有：

- **合規性** – CipherTrust Transparent Encryption 的這項擴充，解決了保護機敏資料的合規要求與法規命令，例如支付卡、健康照護紀錄或者其他機敏資產。
- **防止受到特權用戶的威脅** – 該解決方案提供資料存取控制的加密，讓特權用戶如 Docker 或 OpenShift等群組管理員，能夠像一般用戶執行操作，不會獲得未經授權的機敏資料存取。
- **實現強大的安全性** – 無論容器在資料中心、虛擬環境、甚至是雲端，任何地方儲存或使用，CipherTrust Transparent Encryption for Kubernetes 都將實現強大的資料安全政策。無需對應用程式、容器或基礎架構進行任何變更的情況下，企業可以選擇部署並使用容器以提高成本效益、控制或效能。



特色功能

- **全面的資料安全保障** – CipherTrust Transparent Encryption for Kubernetes 擴展了 CipherTrust Transparent Encryption，讓資安團隊得以在容器內建立資安控制。憑藉這項擴充，您能按照每個容器的狀態一一施行加密、存取控制以及資料存取紀錄。加密可以應用在容器端本地產生並儲存的資料，以及藉由網路檔案系統搭載在容器內的資料。
- **可擴充的透明加密** – 無需對應用程式、容器或基礎架構進行任何變更下，提供資料安全控制。允許對Kubernetes叢集內的所有容器施行單一政策，或是對叢集的每一個容器施行有所區別的不同政策。這項解決方案可因應業務需求變化而擴充或縮小 Kubernetes 環境。
- **細粒度存取控制與可視性** – CipherTrust Transparent Encryption for Kubernetes 提供細部的可視性與控制，滿足最嚴格政策與命令的法規遵循規範。採用 Kubernetes 資安解決方案，企業能依據特定用戶、程序以及容器內的資源組來建立細粒度存取政策。最後，該解決方案能夠在容器之間建立隔離，所以只有經過授權的容器才可以存取機敏資料。

CipherTrust Manager

CipherTrust Manager 是 CipherTrust Data Security Platform 的核心，包括 CipherTrust 透明加密，可集中管理平台上所有產品模組的金鑰、安全策略以及日誌管理。具有虛擬化和實體版本，可用於儲存具有信任根 (root of trust) 的主金鑰。這些設備可以被部署在企業內部，也可以部署在私有或公有雲端基礎架構。

關於 Thales 雲端保護與授權

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