cpl.thalesgroup.com

THALES

Vormetric Data Security Platform
資料表

Vormetric Data Security Platform

隨著資安入侵以驚人的頻率不斷發生，資料保護合規性要求變得越發嚴格，您的組織需要將資料保護延伸至更多的環境、系統、應用程式、流程和使用者中。借助 Thales 的 Vormetric Data Security Platform（Vormetric 資料安全平台），您可以有效地管理整個組織的靜態資料安全。

Vormetric Data Security Platform（Vormetric 資料安全 平台）由一整套產品組成，這些產品建立在通用、 可延伸的基礎架構上，採取高效的集中式金鑰和規則管理。因此，您的安全團隊可以解決資料安全性規則、合規性要求和最佳實務等問題，同時減少管理投入和整體成本。

本平台提供保護和控制資料庫、檔案和容器存取的功能，並且可以保護在雲端、虛擬、大數據和實體環境中的資產。這款可擴充的高效資料安全平台可讓您解決急迫的需求，並為您的組織在出現下一個安全挑戰或合規性需求時做好準備快速回應。

功能

- 對檔案、資料庫和容器進行透明加密
- 應用程式層級加密
- 代碼化
- 動態和靜態資料遮罩
- 通過FIPS 140-2 及 CC 認證的金鑰管理
- 雲端金鑰管理
- 特權使用者存取控制
- 存取稽核記錄
- 批次資料加密和代碼化

環境和技術支援

- IaaS、PaaS 和 SaaS：Amazon Web Services、Google Cloud Platform、Microsoft Azure、Salesforce、Microsoft Office365 和 PCF：Pivotal Cloud Foundry 中的 MySQL 資料庫
- 作業系統：Linux、Windows 和 UNIX
- 大數據：Hadoop、NoSQL、SAP HANA 和 Teradata
- 容器：Docker 和 Red Hat OpenShift
- 資料庫：IBM DB2、Microsoft SQL Server、MongoDB、MySQL、NoSQL、Oracle 和 Sybase 等
- 任何儲存環境

平台特色

- 集中化靜態資料安全性規則
- 管理 Vormetric Data Security Platform（Vormetric 資料安全平台），和第三方廠商加密產品的金鑰
- 跨實體、虛擬、雲端和大數據環境的一致安全性和合規性
- 預先定義的 SIEM 儀表板提供細微、可操作的檔案存取情報
- 靈活性和擴充性可快速支援其他使用案例
- 就資料加密金鑰與受支援的 HSM 和第三方廠商來源整合
- 使用支援的 HSM 作為高保證等級的信任基礎來源（包括 FIPS 140-2 Level 3 認證）

合規性

- PCI DSS
- GDPR
- HIPAA/HITECH
- NIST 800-53
- FISMA
- PIPA
- 區域資料落地和隱私權需求

加強安全性和合規性

透過利用這些靈活、可擴充的解決方案，安全團隊可以處理廣泛的使用案例，並保護整個組織的機密資料。該平台提供全面的功能，讓您能夠滿足一系列安全和隱私權要求，包括支付卡產業資料安全標準（PCI DSS）、一般資料保護規範（GDPR）、健康保險便利及責任法案（HIPAA）、聯邦資訊安全管理法（FISMA）以及區域資料保護和隱私權法律。Vormetric Data Security Platform（Vormetric 資料安全平台）為組織配備了強大的工具，即便資料儲存在雲端或任何外部提供者的基礎架構中，也能應對外部威脅、防範內部濫用並形成持續控制。

將員工和資源效率最大化

Vormetric Data Security Platform（Vormetric 資料安全平台）提供了直覺化以 Web 為基礎的介面、命令列介面（CLI）和應用程式開發介面，包括對 REST API、Java、.Net 和 C 的支援，使管理變得簡單高效。使用這項解決方案，您可以快速一致地對靜態資料套用安全性，將員工效率和生產力最大化。此外，這項高效能解決方案能夠高效利用虛擬和實體伺服器資源，減輕服務傳遞基礎架構的負載。

降低整體擁有成本

Vormetric Data Security Platform（Vormetric 資料安全平台），使靜態資料保護更加簡單、成本更低本平台讓您的 IT 和安全組織能夠以統一、可重複的方式快速保護整個組織的資料。您可以使用

VormetricData Security Platform（Vormetric 資料安全平台）採取一致的集中式方法，而不必使用分散在組織中的大量獨立產品。

平台產品

Vormetric Data Security Platform（Vormetric 資料安全平台）擁有以下產品：

Vormetric Data Security Manager（Vormetricr 金鑰集中管理）。所有 Vormetric Data Security Platform（Vormetric 金鑰安全平台）產品的集中化管理環境。提供規則控制以及加密金鑰的安全生成、管理和儲存。包括以 Web 為基礎的主控台、CLI、SOAP 和 REST API。可作為經 FIPS 140-2 和CC認證的虛擬和實體設備提供。

Vormetric Transparent Encryption（Vormetric 透明加密）。圍繞運行在伺服器上的軟體代理程式構建，可保護內部資料庫、雲端或混合雲端環境中檔案、磁碟區或資料庫中的靜態資料。具有硬體加速加密、最低權限存取控制以及跨資料中心、雲端和混合部署的資料存取稽核記錄等功能。擁有以下延伸模組和新增模組：

- **Container Security。**在 Docker 和 OpenShift容器內部建立控制，由此確保其他容器和處理程序甚至主機作業系統均無法存取機密資料。提供您根據每個容器或在容器內部套用加密、存取控制和資料存取記錄所需的功能。
- **Live Data Transformation（免停機背景加密）。**支援檔案和資料庫的加密和定期金鑰輪換，而不會打擾使用者以及中斷應用程式和業務工作流程— 即使在使用過程中也不會受到影響。
- **Vormetric Transparent Encryption（Vormetric 透明加密）。**支援高效儲存設備。透過加密資料為儲存在儲存系統上的資料提供高度安全性，同時保持重大儲存活動（如重復資料刪除和壓縮）的效率。提供盡可能好的資料保護，同時保持儲存效率— 業界第一的解決方案！
- **Vormetric Transparent Encryption（Vormetric 透明加密）。**支援 SAP HANA。為各種 SAP HANA實作和環境提供進階靜態資料加密、存取控制、金鑰管理和資料存取稽核記錄。

Vormetric Tokenization（Vormetric 代碼化），支援動態資料遮罩。Vormetric Tokenization（Vormetric 代碼化），可讓您輕鬆添加隨機或保留格式的代碼化，以保護資料庫中的機密欄位以及基於規則的動態資料遮罩，從而實現顯示安全性。

Vormetric Application Encryption（Vormetric 應用程式加密）。簡化對現有應用程式中添加 AES 和格式保留加密（FPE）的過程。提供基於各項標準並且可用於執行高效能密碼編譯和金鑰管理作業的 API。

Vormetric Batch Data Transformation（Vormetric 批次資料加密）。使遮罩、代碼化或加密資料庫中的機密資料行資訊變得快速簡單。可在使用 Vormetric Tokenization（Vormetric 代碼化）或 Vormetric Application Encryption（Vormetric 應用程式加密），保護現有機密資料之前使用。提供靜態資料遮罩服務。

Vormetric Key Management（Vormetric 金鑰管理）。提供統一的金鑰管理，以集中管理和安全儲存 Vormetric Data Security Platform（Vormetric Vormetric 資料安全平台）、TDE 以及符合KMIP 的用戶端的金鑰，並安全儲存憑證。

CipherTrust Cloud Key Manager（CipherTrust 雲端金鑰管理）。管理 Salesforce、 Microsoft Azure 和AWS 的加密金鑰，以滿足企業在原生環境之外管理加密金鑰週期方面的合規性和最佳實務需求 – 無需讓企業自身成為密碼編譯的專家可用於私有雲或內部部署。

Vormetric Protection for Teradata Database。讓您能在 Teradata 環境中快速高效地使用強大的靜態資料安全性功能。提供細微保護，支援對 Teradata 資料庫中的特定欄位和資料行進行加密。

Vormetric Security Intelligence（Vormetric 安全資訊記錄）。提供精細記錄，提供檔案存取活動（包括系統管理員存取）的詳細、可稽核記錄。提供與安全性資訊與事件管理（SIEM）系統的整合。提供預先封裝的儀表板和報告，可簡化合規性報告並加速威脅偵測。

Vormetric Data Security Manager（Vormetric 金鑰集中管理）

Vormetric Data Security Manager（DSM）將所有Vormetric Data Security Platform（Vormetric 資料安全平台）產品的管理和規則集中化。DSM 讓組織能夠有效滿足合規性需求、法規要求和行業最佳實務，並隨著部署和需求的變化而作出調整。DSM及其管理的產品與使用者和群組身分識別管理系統（如 LDAP、Active Directory、本地使用者資料庫、Hadoop 和容器環境）整合在一起，提供安全性規則和部署的最佳實務管理。

安全可靠且經 FIPS 認證的系統

為了將執行時間和安全性最大化，DSM 配有備援元件和設備叢集能力，以實現容錯和高可用性。可以實施強有力的職責分離規則，確保一名管理員無法完全控制資料安全性活動、加密金鑰或管理工作。此外，DSM 支援針對系統管理存取權進行雙因素驗證。

靈活的實作選項

所提供的 DSM 為一台 FIPS 140-2 Level 1 虛擬設備以及兩台硬體設備：V6000（FIPS 140-2 Level 2 認證）和 V6100（FIPS 140-2 Level 3 認證）。虛擬設備有與VMware、HyperV、KVM、Amazon WebServices 和 Azure 相容的多種格式。

受支援的 HSM 還可以為虛擬或 v6000 硬體 Vormetric Data Security Management（Vormetric 金鑰集中管理）設備提供 FIPS 140-2 Level 3 認證。

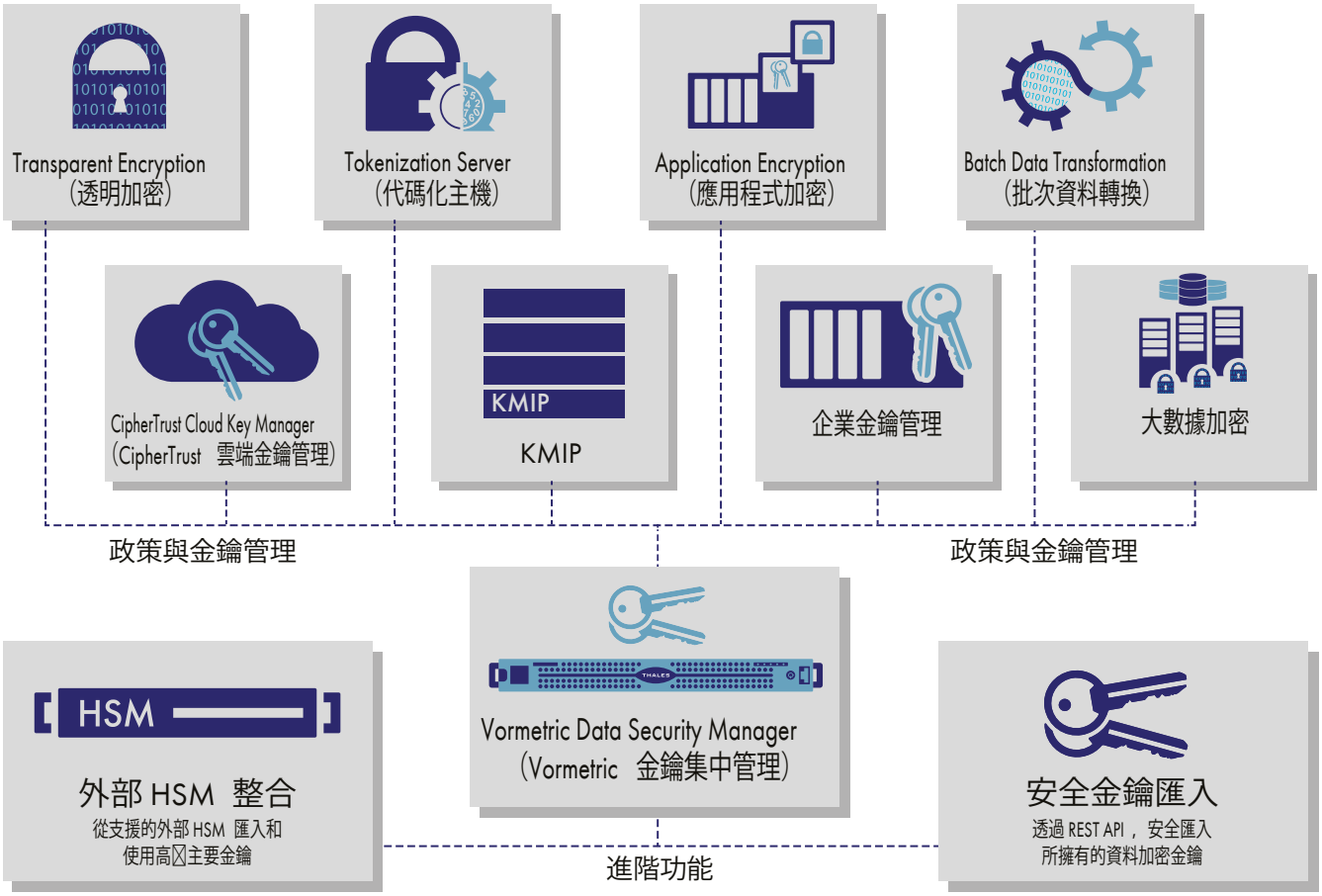
主要功能

- 用於所有平台規則和金鑰管理的單一主控台
- 支援多租戶模式
- 經實證可擴展到 10,000 多個代理程式
- 支援叢集，以實現高可用性
- 工具組和程式設計介面
- 與現有驗證基礎架構輕鬆整合
- 支援 RESTful API
- 多因素驗證和內部 HSM
- 遠端系統管理

技術規格

平台選項：

- FIPS 140-2 Level 1 虛擬設備（可由受支援的外部 HSM 提供 FIPS 140-2 Level 3 認證）
- FIPS 140-2 Level 2 硬體設備（可由受支援的外部 HSM 提供 FIPS 140-2 Level 3 認證）
- FIPS 140-2 Level 3 硬體設備（包括內部 HSM）
- 虛擬設備有與 VMware、HyperV、KVM、Amazon Web Services 和 Azure 相容的多種格式。



在整個混合式企業內實現統一管理

DSM 透過提供各種異質加密金鑰的集中化管理，將資本和費用成本降至最低，這些金鑰包括為 Vormetric Data Security Platform（Vormetric 資料安全平台）產品、IBM Security Guardium Data Encryption、Microsoft SQL TDE、Oracle TDE 和符合 KMIP 的加密產品而生成的金鑰。DSM 具有直覺化以 Web 為基礎的主控台 和 API，用於管理整個企業的加密金鑰、規則和稽核。該產品還將記錄收集進行集中化。

DSM 規格

硬體規格

底座	1U 機架掛接式；17” x 20.5” x1.75”（43.18 cm x 52.07cm x 4.5 cm）寬 x 長 x 高）
重量	V6000: 21.5 lbs (9.8 kg); V6100: 22 lbs (10 kg)
記憶體	16GB
硬碟	配有 FIPS 防篡改密封的雙 SAS RAID 1
序列埠	1
乙太網路	2x1Gb
IPMI	1x10/100Mb
電源供應器	兩個可卸除式 80+ 認證（100VAC–240VAC/50–60Hz）400W
底座入侵偵測	是。另含上蓋的 FIPS 防篡改密封。
最大 BTU	410 BTU（最大）
作業溫度	10° C 至 35° C（50° C 至 95° F）
非作業溫度	-40° C 至 70° C（-40° C 至 158° F）
作業相對濕度	8% 至 90%（無冷凝）
非作業相對濕度	5% 至 95%（無冷凝）
安全機構核准	FCC、UL、BIS 認證
FIPS 140–2 Level 3	V6100 型號配備內部 HSM FIPS 140–2 Level 3 認證， 可透過與受支援的 HSM 整合用於 V6100 和虛擬 DSM
HSM 遠端系統管理	僅限 V6100；需要選配 Remote Administration 套件

軟體規格

管理介面	Secure Web, CLI, REST
管理網域的數量	1,000+
支援 API	PKCS #11, Microsoft Extensible Key Management (EKM), REST
安全驗證	使用者名稱 / 密碼、RSA 多因素驗證（選用）
支援叢集	是
備份	手動和排程安全備份。還原 N of M 的金鑰。
網路管理	SNMP, NTP, Syslog–TCP
Syslog 格式	CEF, LEEF, RFC 5424
認證和驗證	FIPS 140–2 Level 1、FIPS 140–2 Level 2、FIPS 140–2 Level 3 通用標準（ESM PP PM V2.1）

虛擬機器最低規格 — 虛擬設備建議

CPU 數量	2
RAM（GB）	4
硬碟（GB）	100GB
支援精簡佈建	是

Vormetric Transparent Encryption（Vormetric 透明加密）

Vormetric Transparent Encryption（Vormetric 透明加密）提供靜態資料加密服務、中央金鑰控管、特權使用者存取控制及詳細的資料存取稽核記錄，隨時隨地幫助企業組織滿足有關資料保護的合規性報告和最佳實務需求。

該解決方案的透明方法可保護結構化資料庫、非結構化檔案和可從內部係統、多個雲端環境甚至在大數據和容器實作內存取的已連結雲端儲存。實作旨在以最小的中斷、工作量和成本滿足資料安全性需求，可隨選即用 – 即使在部署和推出期間，也能保持業務和作業程序正常進行而不發生變化。

滿足加密和存取控制的合規性需求

加密、存取控制和資料存取記錄為幾乎所有合規性和資料隱私權標準和要求（包括 PCI DSS、HIPAA/Hitech 和 GDPR 等）的基本需求或推薦最佳實務。Vormetric Transparent Encryption（Vormetric 透明加密）提供所需的控制，無需更改作業或業務程序。

可擴充加密

Vormetric Transparent Encryption（Vormetric 透明加密）代理程式在伺服器上的檔案系統或磁碟區層級運行。代理程式可廣泛用於 Windows、Linux、UNIX 平台，可用於實體、虛擬、雲端和大數據環境中，適用於任何基礎儲存技術。管理員透過Vormetric DSM 進行所有規則和金鑰管理。

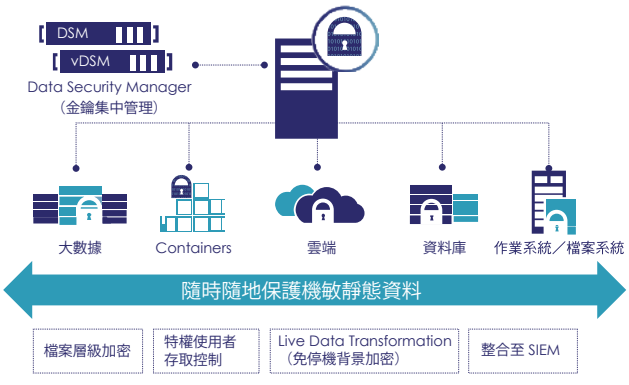
加密在伺服器上進行，消除了傳統上以 Proxy 為基礎的解決方案所面臨的瓶頸。透過利用內建到這類現代 CPU 中的密碼編譯硬體模組（如 Intel AES-NI和 IBM POWER9），性能和可擴充性得到進一步增強。

主要優勢

- 滿足加密和存取控制的合規性和最佳實務需求，可輕鬆跨平台和環境擴展
- 易於部署：無需自訂應用程式
- 制定強有力的保護措施，防止特權內部人員濫用

主要功能

- 業界最廣泛的平台支援：Windows、Linux 和 UNIX作業系統
- 高性能加密：使用內建到主機 CPU 中的硬體加密功能 – Intel 和 AMD AES-NI 和 POWER9 AES 加密
- Suite B 通訊協定支援
- 記錄使用者、應用程式和處理程序的所有已允許、已拒絕和受限存取嘗試
- 基於角色的存取規則控制資料的存取者、存取內容、存取位置和存取方式
- 讓特權使用者在不存取純文字資料的情況下執行工作
- 延伸模組提供了更多功能，包括更細微的容器支援和全面的資料保護，同時保持儲存效率和零停機時間資料加密功能



Vormetric Transparent Encryption（Vormetric 透明加密）隨時隨地保護資料安全

細微的使用者存取控制

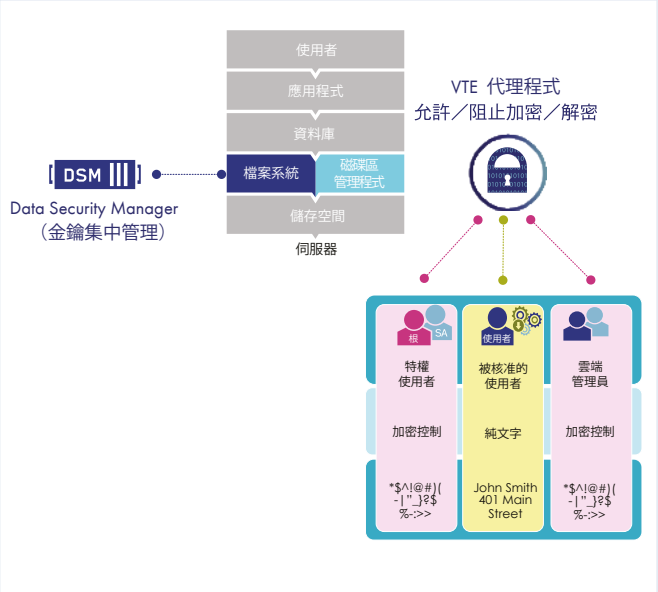
套用設定的細緻、最低權限使用者存取規則，保護資料免於外在攻擊以及特權使用者的誤用。可以對 LDAP/Active Directory、Hadoop 和內容的使用者及群組套用特定規則。存取也能以程序、檔案類型、時間和其他參數進行控制。

非侵入性且易於部署

Vormetric Transparent Encryption（Vormetric 透明加密）代理程式部署在伺服器上的檔案系統或磁碟區層級中，可支援 Linux、UNIX、Windows 檔案系統以及 Amazon S3 和 Azure Files 這類雲端儲存環境。部署時無需更改應用程式、使用者工作流程、業務做法或作業程序。

保護內部或雲端內資料

即使在混合環境部署中，也可以透過管理本地資料中心針對內部資料和雲端資料的加密金鑰和存取規則來控制您的資料。



檔案層級加密可防止特權使用者濫用

技術規格

加密演算法

- AES, 3DES, ARIA

延伸模組授權

- Container Security
- Live Data Transformation（免停機背景加密）
- Efficient Storage（高效能儲存設備）

平台支援

- Microsoft：Windows Server 2019、2016 和 20122
- Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Ubuntu, Amazon Linux
- UNIX: IBM AIX*

資料庫支援

- IBM DB2、Microsoft SQL Server、Microsoft Exchange 資料庫可用性群組（DAG）、MySQL、NoSQL、Oracle、Sybase 等

應用程式支援

- 對所有應用程式（包括 Documentum、SAP、SharePoint、自訂應用程式等）透明

大數據支援

- Hadoop: Cloudera, Hortonworks, IBM
- NoSQL: Couchbase, DataStax, MongoDB
- SAP HANA
- Teradata

加密硬體加速

- AMD 和 Intel AES-NI
- IBM POWER9 密碼編譯副處理器

代理程式認證

- FIPS 140-2 Level 1

Container 支援

- Docker 和 Red Hat OpenShift

雲端支援

- AWS：EBS、EFS、S3、S3I、S3 Glacier
- AZURE：Disk Storage 和 Azure Files
- PCF：Pivotal Cloud Foundry 內的 MySQL 資料庫

**IBM AIX 僅受 Vormetric Transparent Encryption 5.3 版的代理程式支援*

Live Data Transformation（免停機背景加密）

在將純文字轉換為密碼文字，或在為已加密的資料重設金鑰時，靜態資料加密的部署和管理會帶來挑戰。傳統上，這些工作或者需要計劃性停機，或者需要投入大量人力進行資料複製和同步處理工作。Vormetric Transparent Encryption（Vormetric 透明加密）Live Data Transformation (免停機背景加密)的擴充性， 消除了這些障礙，以前所未有的執行時間和管理效率實現了加密和金鑰重設。

免停機加密和金鑰輪換

Live Data Transformation 提供了以下重要功能:

零停機加密部署。該解決方案使管理員能夠加密資料，而不會停機或干擾使用者或者中斷應用程式或工作流程。在加密過程中，使用者和處理程序如常繼續與資料庫或檔案系統進行互動。

無縫、非干擾性的金鑰輪換。安全最佳實務和許多法規要求都需要定期輪換金鑰。Live Data Transformation 使這些需求能夠快速高效地得到滿足。使用該解決方案，您可以執行金鑰輪換，而不必複製資料或將相關應用程式離線。

智慧型資源管理。加密大型資料集可能需要長時間佔用大量 CPU 資源。Live Data Transformation 提供了精細的 CPU 使用量和 I/O 速率管理功能，因此管理員可以在加密和其他業務作業的資源需求之間取得平衡。例如，管理員可以制定一條資源管理規則，規定在上班時間，加密只能消耗 10% 的系統 CPU，而在晚上和週末，加密可以消耗 70% 的CPU。

已建立版本的備份和封存。借助金鑰版本管理，Live Data Transformation 可提供高效的備份和封存復原，從而實現更快的存取。在資料復原作業中，從Vormetric Data Security Manager 復原的已封存加密金鑰會自動應用於較舊的資料集。復原的資料使用當前的密碼編譯金鑰加密。

主要優勢

- 透過零停機時間加密部署提高安全性和資料可用性
- 降低與加密實作和維護相關的成本
- 將加密對使用者體驗的影響最小化
- 利用非干擾性的金鑰輪換來增強安全性和法規合規性
- 加快復原用舊金鑰加密的資料

技術規格

作業系統支援

- Microsoft：Windows Server 2019、2016 和 2012
- Linux：Red Hat Enterprise Linux (RHEL) 6、7 和 8 以及 SuSE Linux Enterprise Server 11、12 和 15

叢集支援

- Microsoft Cluster：File Cluster 和 SQL Server Cluster

資料庫支援

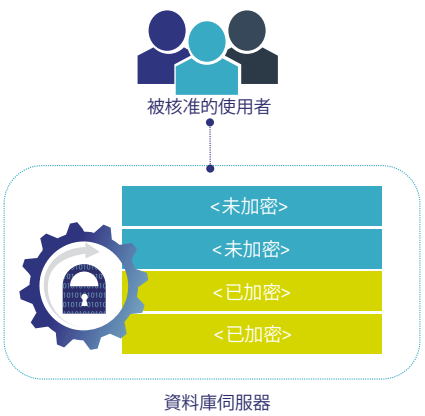
- IBM DB2、IBM Informix、Microsoft SQL Server、Oracle 和 Sybase 等

大數據支援

- Cassandra, CouchBase, Hadoop, MongoDB, SAP HANA

備份 / 複製支援

- DB2 備份、NetBackup、NetWorker、NTBackup、Oracle Recovery Manager (RMAN)、Windows Server 磁碟區陰影複製服務（Volume Shadow Copy Service，VSS）

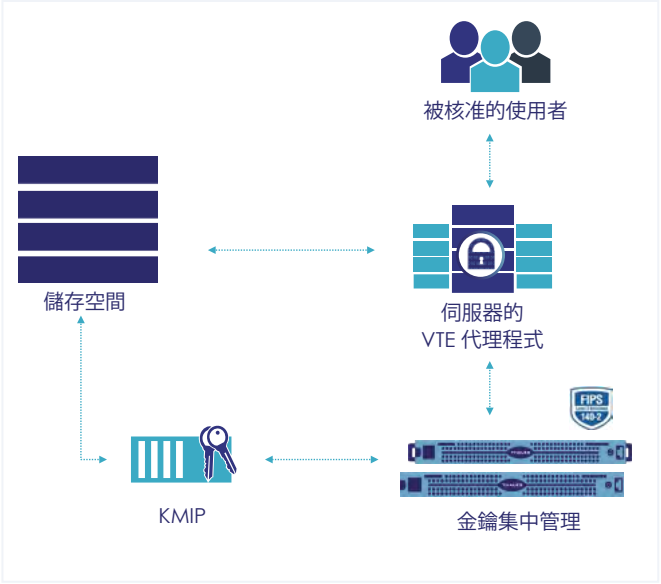


Vormetric Transparent Encryption 的延伸模組和新增模組

Vormetric Transparent Encryption（Vormetric 透明加密）支援高效能儲存設備

借助 Vormetric Transparent Encryption for Efficient Storage（Vormetric 透明加密支援高效能儲存設備）（VTE for Efficient Storage），使用者不再需要在資料安全性和儲存效率之間做出選擇。因為兩者皆可兼得！此解決方案透過加密資料為最終儲存在企業儲存系統上的資料提供高度安全性，同時保持重大儲存活動（如重復資料刪除和壓縮）的效率。VTE for Efficient Storage（VTE 支援高效儲存設備）提供盡可能好的資料保護，同時保持儲存效率— 業界第一的解決方案！

透過在 Vormetric Transparent Encryption（Vormetric 透明加密）和儲存體陣列之間使用安全金鑰共用技術，運行 VTE 的主機上的加密資料現在可以由企業儲存解決方案進行分析，進行壓縮和重復資料刪除，然後以加密格式安全地儲存在陣列上。由此達到兩全其美的效果。



Vormetric Transparent Encryption（Vormetric 透明加密）支援高效能儲存設備

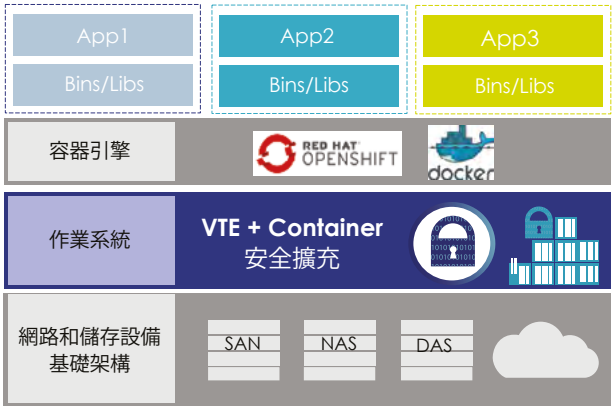
Vormetic Transparent Encryption（Vormetic 透明加密）支援 SAP HANA

Vormetric Transparent Encryption（Vormetic 透明加密）提供了一種經實證的 SAP HANA 資料保護方法，可以滿足嚴格的安全性、資料控管和合規性需求。此方案可以快速部署，無需更改 SAP HANA 或基礎資料庫或硬體基礎架構。利用該方案，組織可以加密 SAP HANA 資料和記錄磁碟區，並建立強有力的管控和實現職責分離。

Vormetric Transparent Encryption Container Security

Vormetric Container Security 將規則導向的 Vormetric Transparent Encryption（Vormetric 透明加密）檔案層級加密、存取控制和資料存取稽核記錄擴充至Docker 和 OpenShift 容器環境中。此方案可提供檔案層級的加密、容器使用者的存取控制，以及在容器映像檔內部儲存資料或由容器映像存取資料，而無需對容器映像檔進行任何更改。

該方案具有符合合規性、法規和最佳實務要求所需的詳細可見度和控制度。細微存取規則提供了容器環境內以及基礎系統層級上的特權使用者存取控制。規則可用於規定機密資料可能的存取者、存取內容、存取位置和存取方式。



容器層級加密

Container Security 技術規格

平台 / 環境支援

- Docker 和 Red Hat OpenShift
- Red Hat Enterprise Linux，8.x
- 可以在實體系統、虛擬機器和 AWS EC2 執行個體上運行EC2 instances

Vormetric Security Intelligence（Vormetric 安全資訊記錄）

Vormetric Security Intelligence（Vormetric 安全資訊記錄）帶來詳細、可操作的安全事件記錄，這些記錄為檔案存取活動提供了前所未有的深入資訊，為預先整合的領先 SIEM 解決方案。根據 Vormetric Transparent Encryption（Vormetric 透明加密）和Vormetric Data Security Manager（Vormetric 金鑰集中管理）提供的資料存取稽核記錄功能，這些資訊可以包括所有關於獲授權資料存取以及任何配置Vormetric Transparent Encryption（Vormetric 透明加密）代理程式的未授權存取嘗試的詳細資料。DSM提供的資訊還包括安全管理員的操作 – 合規性稽核所需的另一項內容。

這些記錄以 SIEM 系統使用的通用格式提供，從 DSM 以及與 SIEM 合作夥伴預先建置的儀表板中集中收集，讓客戶能夠輕鬆地從這些資訊中看到直接價值。儀表板顯示未經授權的存取嘗試，並可用於就未經授權的存取嘗試立即發出警示。

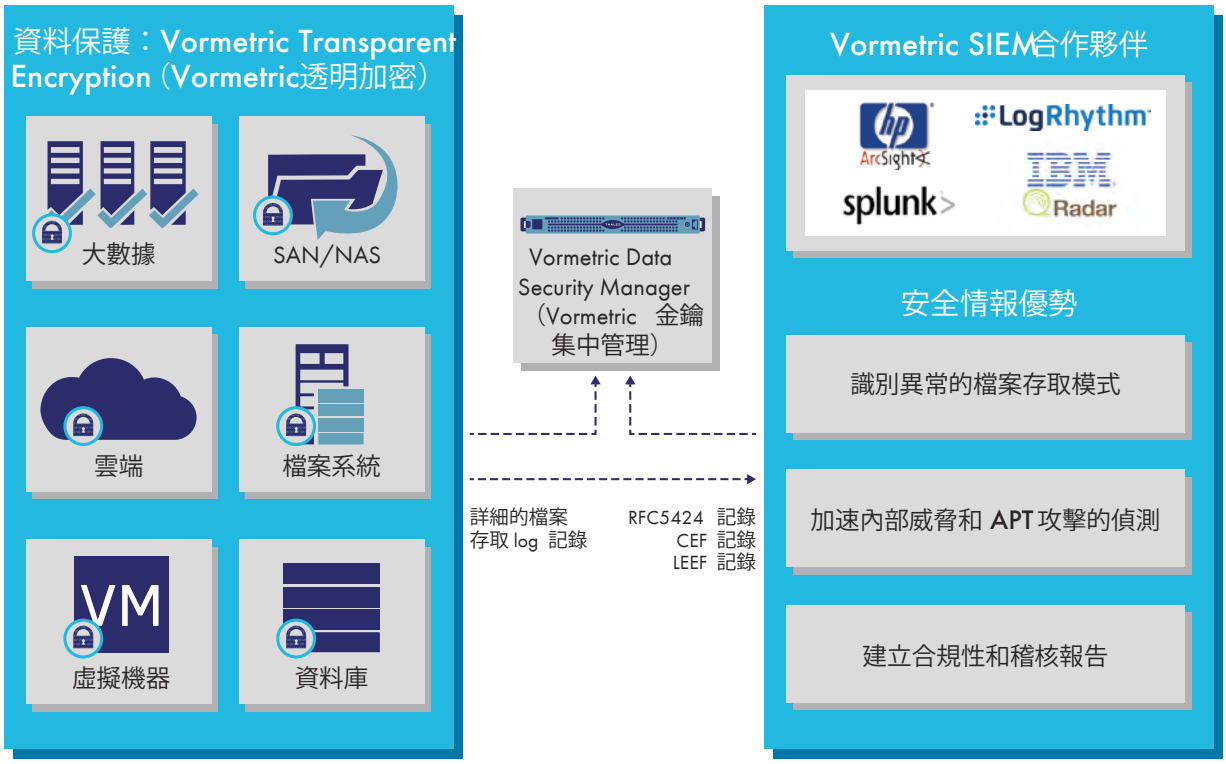
生成的資料集也可用於建立使用者和應用程式存取機密資料的存取模式基準線。這些基準線之後可用於識別可能構成威脅的異常存取模式。

主要功能

- 偵測是否有嘗試未經授權存取的惡意程式碼或惡意內部人員
- 查明使用者存取受保護資料的異常模式，即能表明惡意程式碼（或惡意內部使用者）可能正在竊取資料的模式
- 監測處理程序對受保護資料的存取是否存在異常使用模式，即可能表明某個處理程序已被置入惡意程式碼
- 識別未經授權使用者對 Vormetric Data Security Management（Vormetric 金鑰集中管理）設備的攻擊

SIEM 合作夥伴整合

- FireEye 威脅防禦平台（Threat Prevention Platform）
- Micro Focus ArcSight
- IBM Security QRadar SIEM
- Informatica Secure@Source
- McAfee ESM
- LogRhythm Security Intelligence Platform
- SolarWinds
- Splunk



Vormetric Tokenization（Vormetric 代碼化）支援動態資料遮罩

Vormetric Tokenization（Vormetric 代碼化）支援動態資料遮罩，降低了遵守安全政策和法規要求（如一般資料保護規範（GDPR）和支付卡產業資料安全標準（PCI-DSS））所需的成本和精力。無論機敏資產位於資料中心、大數據環境還是雲端，您都可以對其進行安全保護和匿名。

簡化代碼化

Vormetric Tokenization（Vormetric 代碼化）提供保留格式或隨機的代碼化來保護機密資料規則導向的動態資料遮罩可保護正在使用的資料。RESTful API 與集中式管理和服務相結合，實作每個欄位一行代碼的代碼化。集中式的 Tokenization Server（代碼化主機）管理和設定涉及一個作業儀表板，能在圖形化使用者介面中提供方便的代碼化設定工作流程。

動態資料遮罩。規則定義了是否根據受 AD 或 LDAP伺服器控制的使用者標識碼對欄位進行完全或部分遮罩。

例如，這些規則可以使客戶服務代表只看到信用卡號的最後四位數，而應收帳款工作人員可以查看完整的信用卡號。

非干擾性。格式保留代碼化保護機密資料，而不更改資料庫結構描述。

技術規格

代碼化功能：

- 帶有無法復原選項的格式保留代碼（FF1 或 FF3，英數 / 數字）
- 隨機代碼（英數 / 數字，資料長度高達 128K）
- 日期代碼化
- FPE 和隨機代碼都可以配置為通過Luhn 檢查

動態資料遮罩功能：

- 規則導向，公開的左和 / 或右字元數，帶可自訂的遮罩字元

部署外形規格和選項：

- 開放虛擬化格式（.OVA）和國際標準組織（.iso）
- Microsoft Hyper-V VHD
- Amazon Machine Image (.ami)
- Microsoft Azure Marketplace
- Google Cloud Platform

系統需求：

- 最低硬體要求：4 個 CPU 核心，16-32 GB RAM
- 最低磁碟要求：80GB

應用程式整合：

- RESTful APIs

驗證整合：

- 輕量型目錄存取通訊協定（LDAP）
- Active Directory（AD）
- 用戶端憑證
- OAuth2

性能：

- 在配有 16 GB RAM 的 32 核心伺服器（雙插槽 Xeon E5-2630v3）上，每台代碼伺服器（使用多執行緒和批次（或向量）模式）每秒超過一百萬次信用卡大小代碼化交易

Vormetric Application Encryption（Vormetric 應用程式加密）

Vormetric Application Encryption（Vormetric 應用程式加密）提供金鑰管理、簽名和加密服務，為檔案、資料庫欄位、大數據選擇或基礎架構即服務（IaaS）環境中的資料提供全方位的保護。此解決方案經 FIPS 140-2 Level-1 認證，基於 PKCS#11標準，並以一系列實用且基於使用案例的標準擴展進行完整記錄。Vormetric Application Encryption（Vormetric 應用程式加密）可加快自訂資料安全解決方案的開發。

簡化加密實作

Vormetric Application Encryption（Vormetric 應用程式加密）方案簡化了向應用程式加入金鑰管理和加密作業的過程。開發人員使用與本地 PKCS#11 程式庫相連結的 RESTful API 或者 C、.NET 或基於 Java 的應用程式，為自訂資料安全解決方案新增標準式安全金鑰管理和資料加密服務。

安全的雲端、資料庫和大數據

遵循需要您在應用程式層加密特定欄位的規則和合規性要求， 在機密資料儲存在資料庫、大數據或雲端環境中前予以保護。

技術規格

加密演算法

- AES, 3DES, HMAC-SHA, HMAC MD5, RSA,FPE FF1/FF3

支援的環境：

- 在支援 Web 服務的任何伺服器上的 RESTful API；需要使用 Vormetric Tokenization Server
- Key Services Provider (KSP) for Microsoft Crypto Next Generation (CNG)

OS 和語言和 / 或繫結支援：

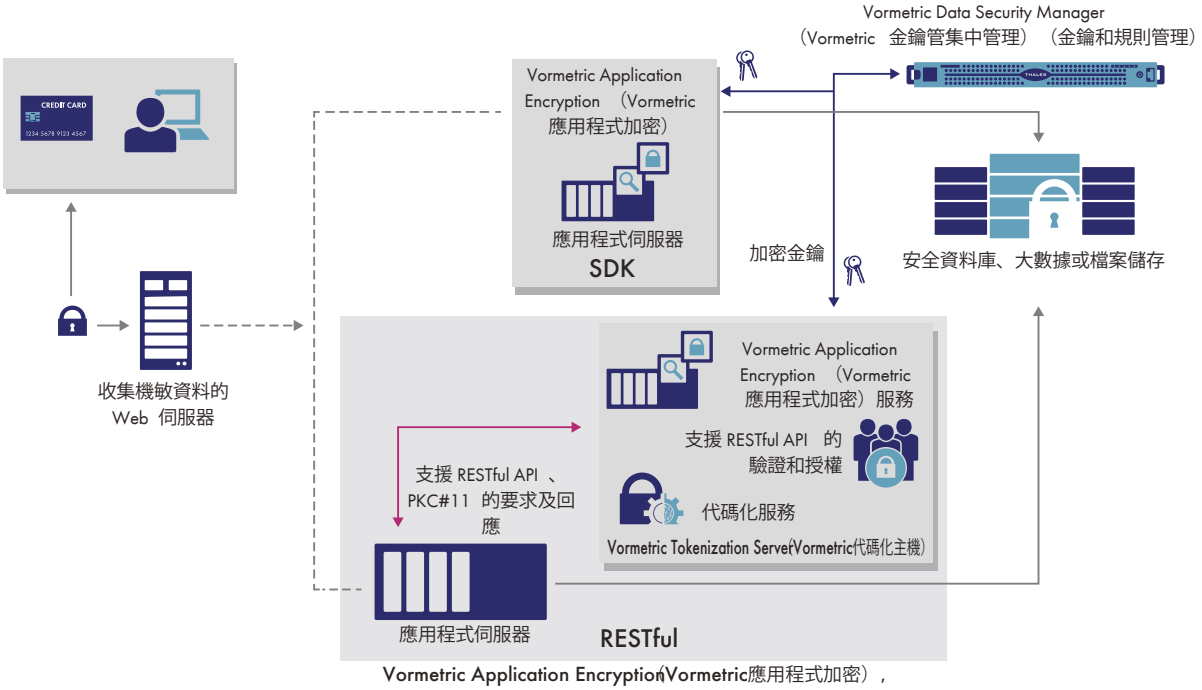
- Windows Server 2008/2012/2016：C、.NET和 Oracle/Sun JDK
- Linux：C 和 Oracle/Sun JDK

安全層

- 職責分離
- 主機註冊和主機級 PIN
- 應用程式層級金鑰存取
- RESTful 使用者名稱和密碼或用戶端憑證
- RESTful 金鑰使用和作業控制

認證：

- FIPS 140-2 Level 1



Vormetric Application Encryption(Vormetric應用程式加密)，
客戶選擇：SDK或 RESTful API

Vormetric Batch Data Transformation（Vormetric 批次資料轉換）

Vormetric Batch Data Transformation（Vormetric 批次資料轉換）提供靜態資料遮罩服務，可支援安全、快速、高效地使用現代數位轉型計畫，例如資料倉儲、內部和雲端的大數據、與 DevOps 共用資料庫以及外包資料分析。

靈活的資料遮罩

Vormetric Batch Data Transformation（Vormetric 批次資料轉換）利用 Vormetric Application Encryption（Vormetric 應用程式加密）和 Vormetric Tokenization（Vormetric 代碼化）支援動態資料遮罩。Batch Data Transformation（批次資料轉換）安裝在已經配備 Vormetric Application Encryption（Vormetric 應用程式加密）的伺服器上，在本地使用 Vormetric Application Encryption（Vormetric 應用程式加密）進行加密和金鑰管理，並與 Vormetric Tokenization Server（Vormetric 代碼化主機）通信以提供代碼化和資料遮罩服務。

數位轉型的資料安全性

轉型方案包括檔案或受支援資料庫的加密或代碼化。使用案例包括：

- 為資料快速重設金鑰
- 與大數據取用者、DevOps 或協力廠商共用安全的資料庫或資料擷取
- 為安全雲端遷移準備資料
- 為代碼化或應用程式層級的加密準備資料庫

主要優勢

- 支援靈活安全的新資料使用
- 加快部署 Vormetric Tokenization（Vormetric代碼化）支援動態資料加密或基於 Vormetric Application Encryption（Vormetric 應用程式加密）的自訂應用程式
- 利用並擴大對 Vormetric Data Security Platform（Vormetric 資料安全平台）的現有投資

技術規格

資料轉換選項：

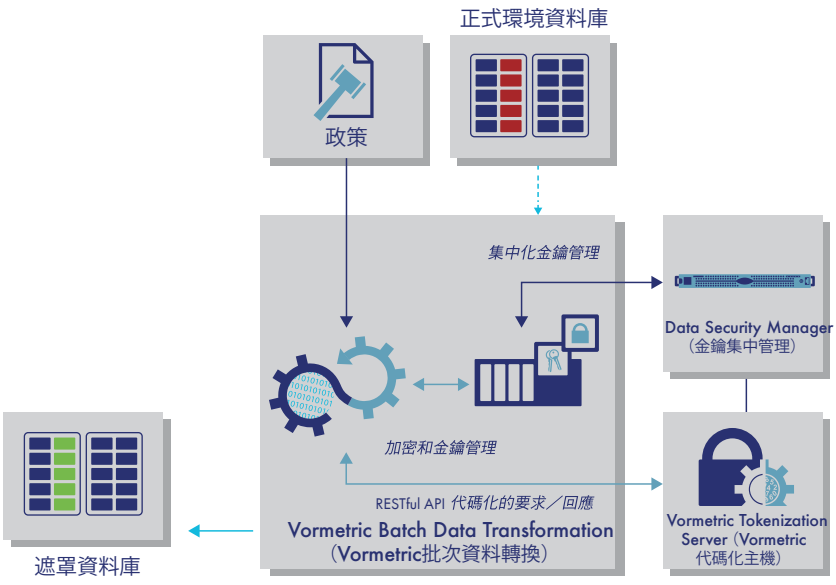
- 代碼化：格式保留 FF1/FF3，隨機代碼化，資料加密：AES 和 FF1/FF3
- 格式保留字母 / 數字

規則檔案選項：

- 每個單獨資料行轉換的具體操作 – 加密、解密、代碼化、去代碼化和重設金鑰
- 無需更改應用程式，輕鬆套用加密
- 靈活的金鑰管理選項 – DSM 或伺服器中的金鑰，多金鑰支援

硬體和作業系統需求：

- 4 核心處理器，16GB RAM（最低）
- Java Runtime Environment (JRE)
- Windows
- Linux – RedHat、CentOS、Ubuntu 和 SUSE



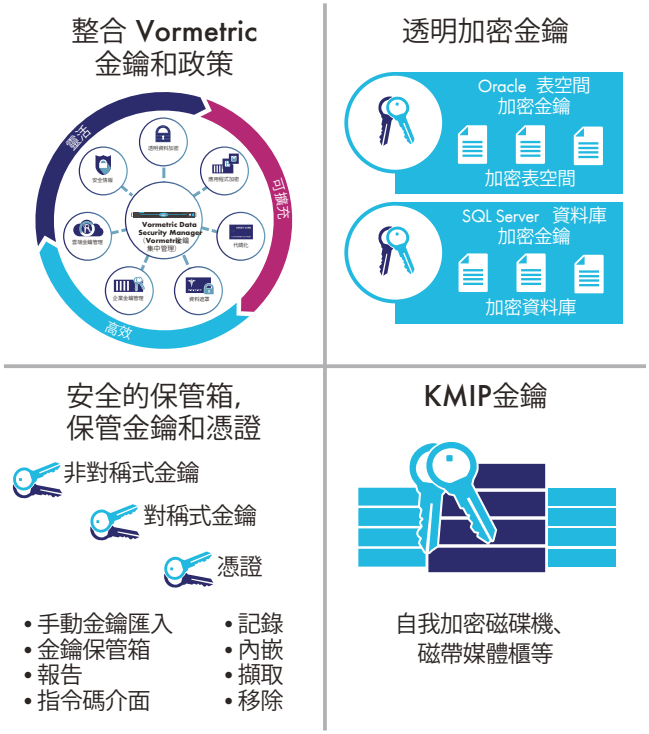
Vormetric Key Management

借助 Vormetric Key Management（Vormetric 金鑰管理），您可以集中管理所有 Vormetric Data Security Platform（Vormetric 資料安全平台）產品的金鑰，並安全地儲存和清查協力廠商設備（包括 IBM Security Guardium Data Encryption、Microsoft SQL TDE、Oracle TDE 和符合 KMIP 的加密產品）的金鑰和憑證。整合金鑰管理可加強跨多個系統實作規則的一致性，並降低培訓和維護成本。

簡化金鑰管理和憑證保存

歷年來，隨著使用加密的應用程式和設備的數量激增，所需的金鑰管理系統的數量也相應增加。金鑰管理系統的不斷增加使得維護高度可用的加密環境變得更加複雜和昂貴。此外，這些完全不同的金鑰管理系統有可能使寶貴的憑證得不到保護，很容易成為駭客的獵物。而且，這些憑證如果不受管控，可能會意外過期，導致重要服務的非計劃停機。

Vormetric Key Management（Vormetric 金鑰管理）使您能夠擴展功能，以便更有效地管理 Vormetric Data Security Platform（Vormetric 資料管理平台）解決方案的金鑰以及第三方廠商產品的金鑰和憑證。此外，CipherTrust Cloud Key Manager（CipherTrust 雲端金鑰管理）使您能夠利用雲端提供商的自帶金鑰服務，同時在金鑰的整個週期中實現對金鑰的完全管控。



建立強有力、可稽核的管控

Vormetric Key Management（Vormetric 金鑰管理）利用 Vormetric Data Security Manager（Vormetric 資料集中管理）進行金鑰的生成和儲存。所提供的 DSM為一台 FIPS 140-2 Level 1 認證虛擬設備以及兩台硬體設備：經 FIPS 140-2 Level 3 認證、配有內部硬體安全模組的 DSM V6100 以及經 FIPS 140-2 Level 2 認證的 DSM V6000。對於雲端的金鑰管理，虛擬 DSM 也適用於 Amazon Web Services，可在 Microsoft Azure Marketplace 上選購。

主要優勢

- 憑證和金鑰的安全儲存
- 憑證和金鑰的到期通知
- 報告可提供狀態和稽核支援

技術規格

管理安全性物件

- X.509 憑證
- 對稱和非對稱的加密金鑰

系統管理：

- 安全的 Web、CLI、API
- 數位憑證和加密金鑰的批量匯入
- 匯入時驗證
- 命令列指令碼

搜索、警示和報告的金鑰和憑證格式

- 對稱加密金鑰演算法：3DES、AES128、AES256、ARIA128、ARIA256
- 非對稱加密金鑰演算法：RSA1024、RSA2048、RSA4096
- 數位憑證（X.509）：DER、PEM、PKCS#7、PKCS#8、PKCS#12

第三方協力廠商加密

- Microsoft SQL TDE、Oracle TDE、IBM SecurityGuardium Data Encryption、KMIP-用戶端
- 合作夥伴列舉：Nutanix、Linoma、NetApp、Cisco、MongoDB、DataStax、華為

API 支援

- PKCS#11、Microsoft Extensible Key Management (EKM)、OASIS KMIP

金鑰可用性和備援

- 透過自動備份跨多個設備安全複製金鑰

CipherTrust Cloud Key Manager（CipherTrust 雲端金鑰管理）

諸多雲端服務提供者提供靜態資料加密功能。然而，許多資料保護要求規定加密金鑰不得由雲端服務提供者儲存和管理。「自帶金鑰」（BYOK）服務和 API 可以滿足這些需求。

客戶金鑰控制

基於 BYOK 的客戶金鑰控制允許分離、建立、擁有和控制（包括撤銷）加密金鑰或用於創建它們的租用戶機密。CipherTrust Cloud Key Manager（CipherTrust 雲援金鑰管理）利用 BYOK API，可透過集中管理、以可見的方式為客戶提供加密金鑰的全週期控制，降低金鑰管理的複雜性和運營成本。

強大的加密金鑰安全性

客戶金鑰控制需要安全地生成和儲存金鑰。CipherTrust Cloud Key Manager（CipherTrust 雲端金鑰管理）利用 Vormetric Data Security Manager（Vormetric 金鑰集中管理）或所支援的 HSM 的安全性來建立和儲存金鑰。

IT 效率和合規性工具

在單一瀏覽器視窗中為多個雲端提供商集中管理金鑰、自動輪換金鑰以及支援受支援的雲端同盟登入和原生雲端金鑰管理，這些功能可共同提高 IT 效率。CipherTrust Cloud Key Manager（CipherTrust 雲端金鑰管理）雲端記錄和預先封裝的報告可支援快速合規性報告。

符合您需求的實作選擇

CipherTrust Cloud Key Manager（CipherTrust 雲端金鑰管理）提供了多種方便的實作選擇，可滿足您的安全性和部署需求：

- 所有軟體均具備經 FIPS 140-2 Level 1 認證的金鑰安全性。CipherTrust Cloud Key Manager Virtual Appliance（CipherTrust 雲端金鑰管理虛擬設備）和虛擬 Data Security Manager（Vormetric 金鑰集中管理）都可以在 Amazon Web Services 和Microsoft Azure 中具體時顯，或者部署在任何使用 VMware 的公有或私有雲中。
- 需要 FIPS 140-2 Level 3 或 2 的客戶可以在內部或託管資料中心部署或利用現有的 Vormetric Data Security Manager（Vormetric 金鑰集中管理）設備或所支援的 HSM。

主要優勢

- 透過全週期雲端加密金鑰管理，發揮「自帶金鑰」服務的價值。週期控制包括基於基本或「到期時」排程的自動化金鑰輪換、受支援雲端的雲端原生金鑰管理以及全動態金鑰中繼資料管理。
- 透過 FIPS 140-2 Level 3 經驗證的金鑰建立和儲存，遵循最嚴格的資料保護要求
- 透過跨多個雲端環境的集中金鑰管理提高 IT 效率

支援的雲端環境

- IaaS 和 PaaS：Microsoft Azure、Azure China 和Germany National Cloud、Microsoft Azure Stack、Amazon Web Services
- SaaS: Microsoft Office365, Salesforce.com, Salesforce Sandbox

Vormetric Protection for Teradata Database（Vormetric 支援保護 Teradata 資料庫）

透過在 Teradata 環境中彙總大量企業資料，企業可以獲得前所未有的洞察力和戰略價值。不幸的是，這種資料彙總也會帶來前所未有的風險。如果沒有適當保護，在這些環境中編譯的機敏資產可能會被特權管理員無意中公開，或者成為惡意內部人員和外部攻擊者竊取的對象。如今，Vormetric 能讓您的組織防範這些風險。Vormetric Protection for Teradata Database（Vormetric 支援保護 Teradata 資料庫）讓您能在 Teradata 環境中快速高效地使用強大的靜態資料安全性功能。

加強安全性，同時將中斷和成本最小化

Vormetric Protection for Teradata Database（Vormetric支援保護 Teradata 資料庫）簡化了保護機敏記錄的過程，支援對 Teradata 資料庫中的特定欄位和資料行進行加密。此解決方案還提供了經 NIST 認可的格式保留加密（FPE）功能，因此您可以加密機敏記錄，無需更改其格式或欄位結構描述。這不僅會使加密對相關應用程式和工作流程的潛在影響降至最低，而且有助於您避免傳統加密方法帶來的儲存需求增加。而且，此方案可提供動態資料遮罩，使您能夠向不同的使用者提供不同的解密級別和呈現相應資料。此外，您可以在 Teradata Appliance for Hadoop（Teradata 支援的 Hadoop 應用程式）上安裝 Vormetric Transparent Encryption（Vormetric透明加密）代理程式，將保護範圍從 Teradata 資料庫擴展到 Teradata 大數據分析。

主要優勢

- 提高安全性的同時不影響大數據分析的價值
- 提供保護措施，防止特權使用者的網路攻擊和濫用
- 快速部署

主要功能

- 實現高性能，根據 Teradata 節點的數量進行擴展
- 利用 FPE，最大限度減少儲存增長和加密中斷
- 用於加密、代碼化、動態資料遮罩和解密的使用者定義函式（UDF）可以輕鬆整合到現有 SQL 代碼中
- 不同資料行使用不同的金鑰加密
- 支援 ASCII 文本和 Unicode，提供靈活的語言和技術支援
- 經認證的 Teradata 加密解決方案

技術規格

加密演算法

- AES, FPE (FF1, FF3)

支援的平台：

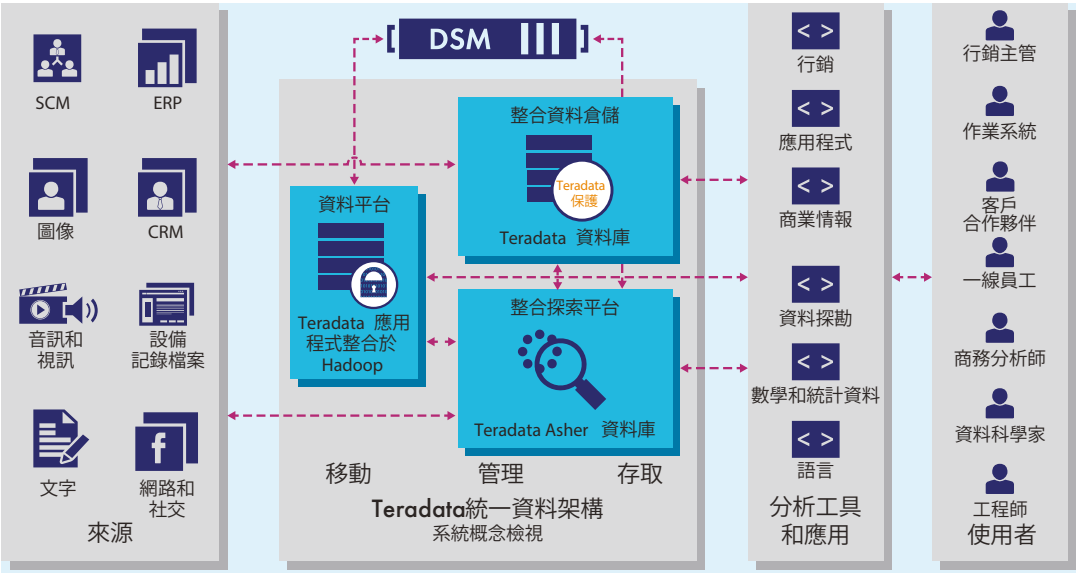
- Teradata 資料庫，版本 16.20 及更低版本，取決於 SLES 和產品版本

作業系統：

- SUSE Linux Enterprise Server (SLES)，版本 10 或 11

最大資料行寬度：

- ASCII: 16KB
- Unicode UDFs: 8KB



簡化加密部署和使用

此方案透過提供可用於執行密碼編譯和金鑰管理作業的文檔化、標準式的應用程式開發介面（API）和使用者定義函式（UDF）來降低開發人員的作業複雜度。借助該方案，Teradata 使用者可以設定自己可設定的設定檔以便提交加密和解密要求，包括從標準的 AES 加密和 FPE 中進行選擇。

支援集中式金鑰和規則管理

Vormetric Protection for Teradata Database（Vormetric 支援保護 Teradata 資料庫）與經 FIPS 認證的強化管理和金鑰儲存設備 Vormetric Data Security Manager（DSM）無縫配合。借助 DSM，您可以對 Vormetric Protection for Teradata Database（Vormetric 支援 Teradata 資料庫）和 Teradata Appliance for Hadoop（Teradata 支援 Hadoop 應用程式系統）、其他 Vormetric Data Security Platform（Vormetric 資料安全平台）解決方案和協力廠商加密產品的金鑰和存取 規則進行集中管理。

THALES

Thales 台灣辦公室
114 台北市內湖區瑞湖街 88 號 4 樓之 3（亞太經貿廣場C樓）
電話+886 2 7745 1888
傳真+886 2 2658 3922
E-mail: apacsales.cpl@thalesgroup.com

> cpl.thalesgroup.com <