Entrust DataControl

數據加密、多重雲端密鑰管理及工作負載安全

重點

- 工作負載全生命週期加密管理
- 企業密鑰管理伺服器 (KMS)
- 強大而精細的虛擬機器 (VM) 加密：實時啟動 (OS) 及數據區隔加密
- 存取管理員職能分工控制
- 完美整合至 Entrust nShield® HSM，以獲取 FIPS 140-2 三級認證信任根

管理加密工作負載可能會十分複雜，尤其是在多重雲端環境中

工作負載從預備到部署，以至備份到最終結束，需經歷多個生命週期。各階段都會面臨不同的潛在數據盜竊或其他濫用風險。

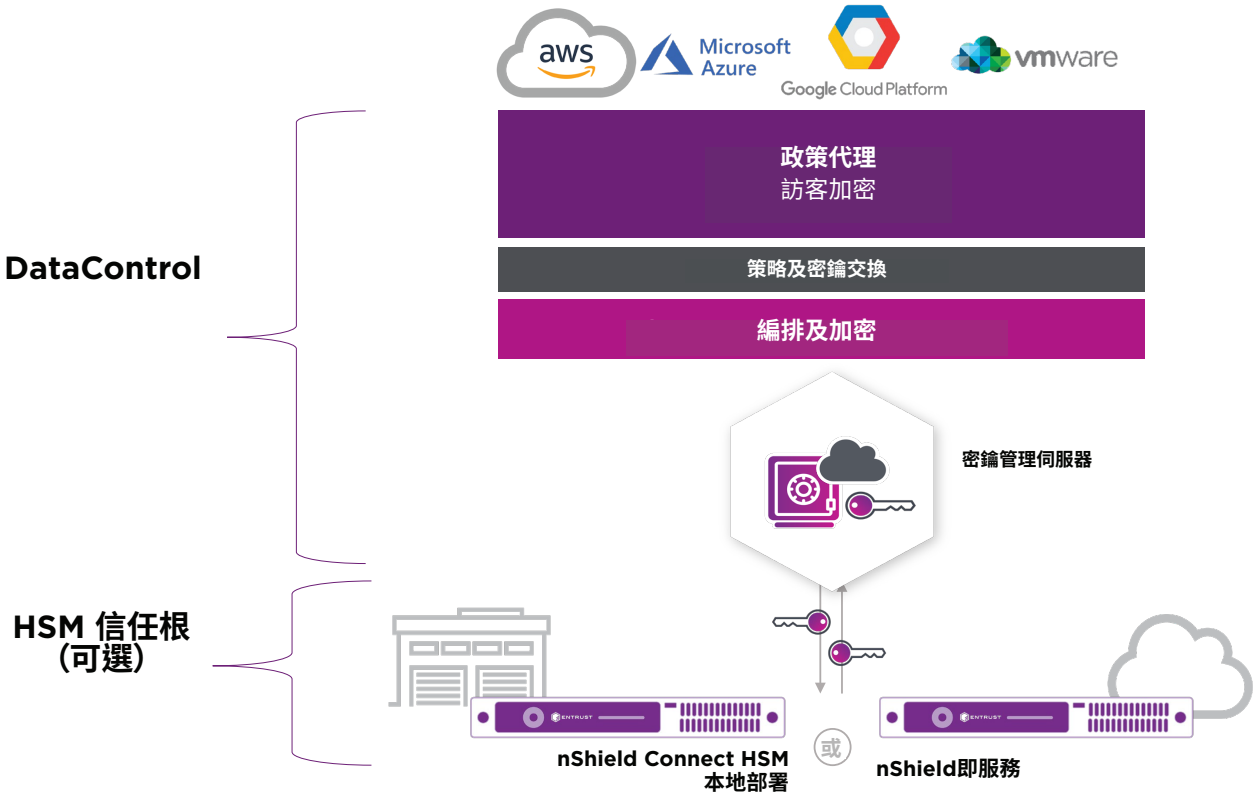
工作負載加密並非部署一次便可安枕無憂的操作

頻繁輪換數據加密的密鑰至關重要。透過各雲端供應商平台管理工作負載加密不單複雜，而且亦會增加政策不一致及人為錯誤風險。內置的密鑰管理策略能減低複雜性並確保一致性。

Entrust DataControl（前稱 HyTrust）在整個生命週期內保護多重雲端工作負載，並降低跨雲端平台進行工作負載保護的複雜性。這為企業的關鍵及敏感資訊提供更周全的保護，並確保遵守數據私隱條例。

在 entrust.com 上了解更多關於 DataControl 的資訊

Entrust DataControl



支援部署平台

- CentOS
- Red Hat 企業版 Linux
- Ubuntu
- SUSE Linux Enterprise Server
- AWS Linux
- Windows Server Core 2012 R2 版、2016 版及 2019 版
- Windows Server 2012 版、2012 R2 版、2016 版及 2019 版
- Windows 8.1 及 10

部署媒體

- ISO
- OVA (開放式虛擬設備)
- 可通過 Amazon Marketplac 獲取 Amazon Machine Image (AMI)
- 可通過 Microsoft Azure Marketplace 獲取 Virtual Hard Disk (VHD)

在 entrust.com 上了解更多關於 DataControl 的資訊

Entrust DataControl

主要功能及優勢

在多重雲端基礎建設中管理加密工作負載

DataControl 讓你能於不同的基礎建設上管理加密工作負載，包括通過本地設備及領先的公用雲端平台進行管理。通過 DataControl，你可獲得集中且可調式的解決方案，控制所有的加密密鑰。DataControl 包含 VMware 認證的 Entrust KeyControl 密鑰管理伺服器 (KMS)。

深度工作負載保護

DataControl 提供精細加密保護，帶來更高安全性。VM 屬獨立加密，其對數據的保護不限於管理程式或數據庫存。在 VM 內，各分區可獲分配獨一無二的密鑰以用作加密，包括驅動 (OS) 硬盤及交換分區。

輕鬆部署及管理

DataControl 讓你透過單一界面靈活部署所有工作負載加密，消除單獨使用各平台加密功能的複雜性。

- 優越用戶體驗
- 零停機加密
- 利用高可用集群確保故障恢復能力

存取控制

DataControl 提供以政策為基礎的強大存取控制功能，執行用戶職責劃分。透過對加密卷執行存取控制，防止根用戶或系統管理員存取敏感數據。

支援刪除重複數據

過往，由於加密數據會令各數據區塊有所不同，故人們擔心加密及刪除重複數據無法並存。DataControl 的獨特方案可提供 AES 256 位元加密，同時保持刪除重複數據功能的 91% 儲存空間優勢。

支援平台

- **私有雲平台：**
  - vSphere
  - OVHCloud
  - VxRail
  - Pivot3
  - NetApp
  - Nutanix
- **公共雲平台：**
  - Amazon Web Services (AWS)
  - IBM Cloud
  - Microsoft Azure
  - VMware Cloud (VMC) on AWS
  - Google Cloud Platform (GCP)
- **支援管理程序：**
  - ESXi
  - AWS
  - Azure
  - KVM
  - GCP

在 entrust.com 上了解更多關於 DataControl 的資訊

Entrust DataControl

技術規格

- 加密啟動 (OS)、交換及數據分區
- 支援加密 Windows GPT 驅動器，包括 UEFI Secure Boot 驅動器
- 各分區設有獨立密鑰
- 具備Intel硬件加速支援的強大 AES (128/256 位元) 加密
- 符合 FIPS 140-2 的一級加密密鑰管理。完美整合至 Entrust nShield FIPS 140-2 三級硬體安全模組
- 通過自動重新加密功能達致零停機加密
- 為 Windows VM 而設的動態分區大小調整
- 支援高可用性 (HA)，備有主動 — 主動數據集群，各集群最多可設定 8 個 KMS 伺服器
- 支援刪除重複數據的單一加密密鑰
- 通過 VMware vSphere 及 vSAN 加密認證
- 建基於 REST、用於 DevOps 的 API 整合
- 保護加密工作負載，選用啟動及複製保護技術，避免未經授權的存取

DataControl 為數據加密、多重雲端密鑰管理及虛擬機器與容器化工作負載安全政策合規產品套件的一部分。詳情請參閱下方表格。

ENTRUST 產品	描述	額外資訊
KeyControl BYOK	用於產生你專屬的加密密鑰並於 AWS、Microsoft Azure 或 Google 雲端平台上使用	使用獨立授權或透過 KeyControl 及/或 DataControl 進行部署
KeyControl	為支援 KMIP 工作負載而設的企業加密密鑰管理	使用獨立授權或透過 KeyControl BYOK 及/或 DataControl 進行部署
DataControl	用於多重雲端環境中虛擬機器加密的精細、基於代理的控制與加密密鑰管理	使用獨立授權或透過 KeyControl 及/或 KeyControl BYOK 進行部署
CloudControl	符合用於虛擬化及容器化環境中的自動化工作負載安全政策實施，保護敏感數據免遭雲端設定錯誤威脅。	

了解更多
entrust.com

ENTRUST
全球總部
1187 Park Place, Minneapolis, MN 55379
免費美國電話：888 690 2424
國際長途電話：+1 952 933 1223