Trusted Cyber Technologies

THALES

Protecting Data with Thales Key Management and Dell EMC VxRail HCI System

The Challenge

The challenges inherent in securing IT data environments today are multiple:

- increase in regularity and sophistication of data breaches
- data privacy/compliance mandates (e.g. FIPS, HIPAA, GDPR, PCI-DSS, etc.)
- cost control
- rapid digital transformation
- explosive data growth

To meet these challenges, a data-centric solution that reliably secures sensitive data as it moves from endpoints through networks to applications and the cloud is required. Data protection through proven encryption and centralized, scalable management of encryption keys is the last bastion of protection. Fortunately, Thales and Dell Technologies integrated solutions work at a lower total cost of ownership (TCO) to provide comprehensive data security and enable compliance in today's environment

The Solution

Using the industry standard Key Management Interoperability Protocol (KMIP), Dell EMC VxRail HCI systems integrate with Thales enterprise key management (EKM) to mitigate the threat of unauthorized access to encrypted data, at vSAN or VM-level (see Fig. 1, below). Thales EKMs provide security by storing and managing keys away from encrypted devices and data, thus securing keys (and, thereby, data) even if the storage system is compromised. Thales EKM is available for sale to the U.S. federal government exclusively through Thales Trusted Cyber Technologies.

There are two Thales EKMS deployment options available

- **Encryption at the VM level**: (see Fig. 2) Encryption of the entire VM, including all the files within the container. Everything remains encrypted, even as VMs are moved and re-deployed. Requires one KMIP license per vCenter server. Thales Luna Hardware Security Module (HSM) maintains Root of Trust (RoT) security as it provides data encryption key pairs for each VM. Higher security than VSAN-level encryption. Deduplication and compression is not available with this deployment option.

- **Encryption at the VMWare vSAN level**: (see Fig. 3) Each virtual disk in the vSAN is encrypted, protecting all data at rest. Requires one KMIP license per server and one license per ESXi server. Luna HSM provides secure data encryption key pairs per virtual disk. This deployment option enables the addition of deduplication and compression.

Additionally, Thales EKM simplifies and centralizes encryption key policies and management and enables regulatory compliance through:

- role-based access control to keys and policies
- multi-tenancy support with ultimate separation of duties
- robust auditing and reporting of all key management operations
- Root of Trust security available through a portfolio of Hardware Security Modules (HSM), with internal and external models that offer options of FIPS compliance Level 1, 2 or 3
- support for turnkey encryption at application, file, data, or database level. Support for data within VM and Container

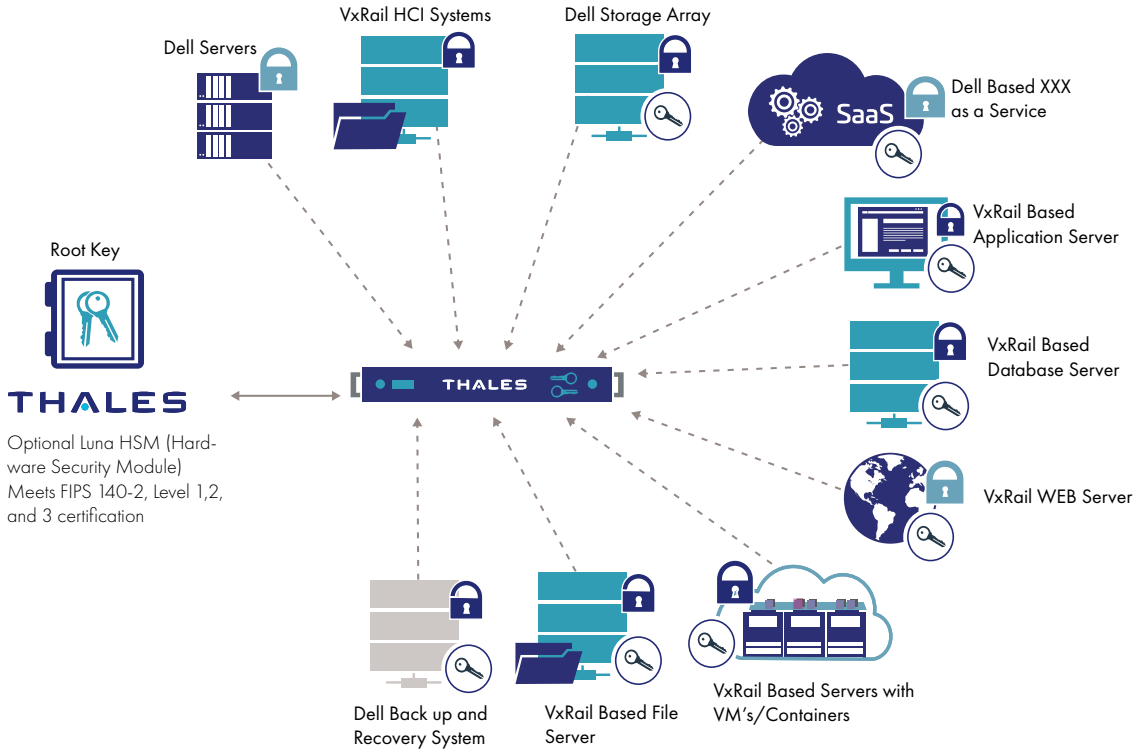

Fig. 1 - Thales Enterprise Key Management solutions and DELL Technologies and 3rd party platforms

Security at a Lower Total Cost of Ownership (TCO)

With Thales and Dell, the cost of key management is distributed amongst multiple appliances, rendering the prohibitive cost of expensive, dedicated point products with disparate features and user interfaces a thing of the past. Whether the data is stored in applications, databases, files, virtual machines (VMs), containers, or storage appliances, Thales EKMs lower the cost of key management and encryption through centralized administration and automated operations across multiple encryption deployments and products. Thales EKMs reduce the additional staff and time it takes to integrate and manage multiple systems, minimizing complexity, costs and the chance for user errors to contribute to the breach of valuable data. Thales EKM protects data across the entire organization in a central, automated, uniform and repeatable way, freeing IT staff and budget for the next security challenge and new compliance requirement.

Key Capabilities

- Centralized Key Management with the Largest Ecosystem of Partners. Centralized key management for multiple on- premises data stores and cloud infrastructures.
- Full Key Lifecycle Management and Policy Driven Automated Operations: Simplifies management of encryption keys, automates policy-driven operations and generates custom alarms
- Centralized Administration and Role-Based Access Control: Role-based access control using existing AD and LDAP credentials

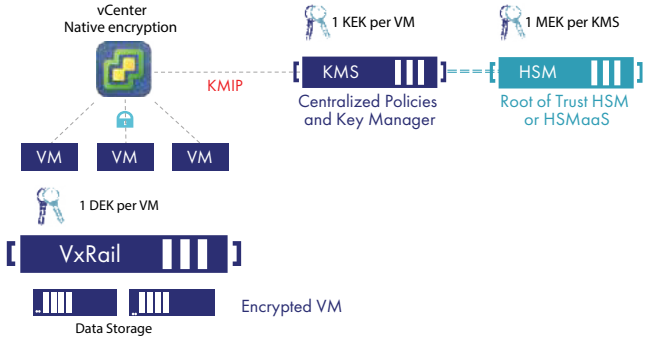

Fig. 2 Encryption at the VM level

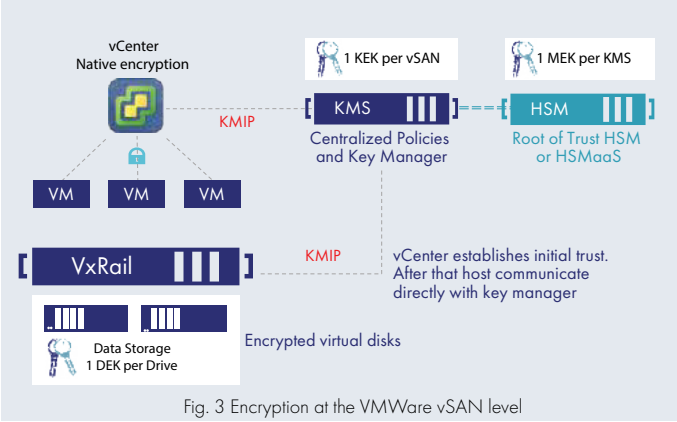

Fig. 3 Encryption at the VMWare vSAN level

Fig. 3 Encryption at the VMWare vSAN level

- Robust Non-Repudiation Auditing and Reporting (integrates with popular SIEM tools): Track all key state changes, administrator access, and policy changes in multiple log formats (RFC-5424, CEF, LEEF) allowing easy integration with popular SIEM tools. Generates customizable email-based alerts.
- High Availability Clustering. Supports high availability to mission-critical workloads
- Multi-tenancy support. Ideal for a large organization with a distributed location or service provider
- High-speed Interfaces with NIC Bonding Optional 2x1GB/2x10GB network interface cards (NIC) as well as NIC bonding to increase available bandwidth.
- Password and PED Authentication: Choice of password or PIN Entry Device (PED) authentication

Available Thales EKMs

Thales Enterprise Key Management Platforms

Features	Physical Appliances	Virtual Appliances
Max Keys	1,000,000	25,000
Max concurrent clients per cluster	1,000	1,000
FIPS 140-2 Support	L2 L3 with an external or build-in HSM	L1 L3 with an external HSM
Supports the SafeNet Data Protection Portfolio	Yes	Yes
Redundant hot-swap HDs & Power	Yes	N/A
Example of Thales Offering	CipherTrust Manager K470 (without HSM), K570 (with HSM), CipherTrust Manager V6000 (without HSM) and V6100 (with HSM)	CipherTrust Manager K170V, CipherTrust Manager virtual version

The Dell Technology Partner Program

Thales is a Dell Technology Partner and is approved by Dell to run on various Dell platforms. The Dell Technology Partner Program is a multi-tier program that includes ISVs, IHVs and Solution Providers. This global program helps partners build innovative and competitive business solutions using Dell Storage platforms.

https://www.dellemc.com/partner/en-us/partner/partner.htm

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com