cpl.thalesgroup.com

DELL Technologies | THALES Building a future we can all trust

Thales CipherTrust Enterprise Key Management and Dell Technologies

The Challenge

Data encryption is fundamental to any defense-in-depth strategy whether the goal is to protect sensitive data from unauthorized disclosure or satisfy compliance mandates. Data is the new "gold," and as value of data grows so does the urgency to protect it. This is driven by:

1. Data Privacy/Compliance Mandates:

Organizations must demonstrate their control over all sensitive data when it moves across or out of their domain, by satisfying an ever-increasing number of government or industry compliance mandates. Such mandates include FIPS, HIPAA, GDPR, PCI-DSS, DPA, APPI, etc.

2. An Increasing Number and Sophistication of Data Breaches:

Growing risks from sophisticated cyber attackers who can easily bypass existing network or endpoint defenses and steal sensitive data, negatively impacting your company's brand reputation and share price.

3. Collocation of Encryption Keys with Encrypted Data:

Hackers can gain unauthorized access to sensitive data if they can somehow gain access to keys located in the same place, when native encryption mechanisms are used.

Data protection through proven encryption and centralized, scalable management of encryption keys has become the last bastion of protection for most enterprises. Fortunately, organizations can count on Thales and Dell integrated solutions to provide comprehensive data security.

The Solution

Using the industry standard Key Management Interoperability Protocol (KMIP), Dell integrate with Thales CipherTrust Enterprise Key Management (EKM) to mitigate the threat of unauthorized access to encrypted data.

Thales CipherTrust EKM provides external key management and data encryption for multiple product lines from Dell and 3rd party platforms, enabling you to satisfy compliance mandates and keeps your sensitive data secure, even in the event of a breach. By storing keys away from encrypted devices and the data residing in storage arrays, file-systems, databases or applications, Thales CipherTrust EKM ensures that encrypted information is protected from unauthorized access.

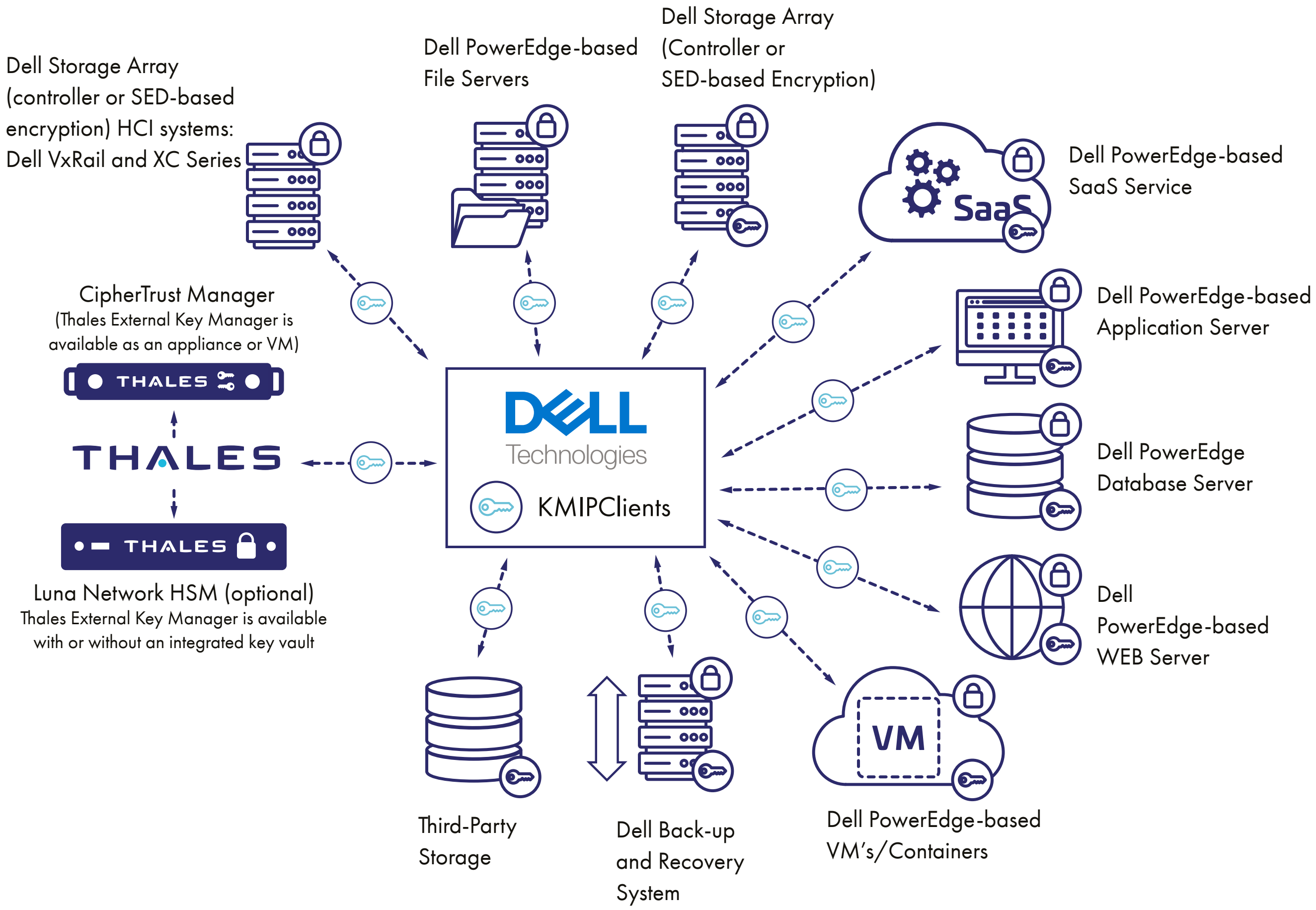
Dell Storage Array (controller or SED-based encryption) HCI systems: Dell VxRail and XC Series
Dell PowerEdge-based File Servers
Dell Storage Array (Controller or SED-based Encryption)
Dell PowerEdge-based SaaS Service
SaaS
CipherTrust Manager (Thales External Key Manager is available as an appliance or VM)
THALES
THALES
Dell PowerEdge-based Application Server
DELL Technologies
KMIPClients
Dell PowerEdge Database Server
THALES
Luna Network HSM (optional) Thales External Key Manager is available with or without an integrated key vault
Dell PowerEdge-based WEB Server
VM
Third-Party Storage
Dell Back-up and Recovery System
Dell PowerEdge-based VM's/Containers

Figure 1 – KMIP enabled interface between Thales CipherTrust EKM solutions and Dell and 3rd party platforms (Thales EKM is tested and validated with PowerEdge servers with an out-of-the-box licensing option available through Dell)

Benefits of Thales CipherTrust Enterprise Key Management

Thales CipherTrust EKM solutions provide Dell customers with complete control by securing the keys needed to access the storage system, and offer benefits such as:

- **Centralized Administration of Granular Access, Authorization Controls and Separation of Duties -** Unify key management operations across multiple encryption deployments and products, while ensuring administrators are restricted roles defined for their scope of responsibilities, from a centralized management console.
- **Full Lifecycle Key Support and Automated Operations -** Manage key life-cycle (key generation, distribution, deactivation, deletion, storage, and backup) for a variety of systems, application servers, databases, and file servers, and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.
- **Simplified Compliance -** Save staff time while satisfying compliance mandates with efficient, centralized auditing of key management practices such as FIPS 140-2, PCI-DSS, HIPAA, GDPR.
- **High-Availability and Intelligent Key Sharing -** Deploy in flexible, high-availability configurations in data centers or in the cloud across geographically dispersed centers or service provider environments using an active-active mode of clustering.
- **Centralized Auditing and Logging -** Detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation and can be consumed by leading 3rd party SIEM tools.
- **Lower Administration Costs -** Lower the cost of key management and encryption with centralized administration and automated operations.
- **Physical and Virtual Appliance -** Thales CipherTrust Manager is available as either a virtual appliance or hardened physical appliance.
- **Risk Mitigation with Maximum Key Security -** Tamper-proof hardware security module (HSM) options supporting a hardware root of trust. k570 CipherTrust Manager hardware appliance is equipped with a hardware security module (HSM), and is FIPS 140-2 Level 3 compliant.

The foundation for Thales Enterprise Key Management solutions: CipherTrust Manager

CipherTrust Manager is a high-availability appliance that centralizes encryption key management for Thales Data Security Products and third-party encryption solutions. The appliance manages key lifecycle tasks including generation, rotation, destruction, import and export.

CipherTrust Manager additionally enhances key management by providing convenient back-up services and delivering strong separation of duties for increased security. CipherTrust Manager can be separated into logical entities, or domains, dedicated to unique key management environments, providing additional security and ultimate separation of duties, where no single administrator has access to all domains.

CipherTrust Manager is available as either a hardware or a virtual appliance. The k470 CM hardware appliance is FIPS 140-2 Level 2 compliant and the k570 CM hardware appliance, equipped with a hardware security module (HSM), is FIPS 140-2 Level 3 compliant. The virtual appliance is certified to FIPS 140-2 Level 1.

The following provides a side-by-side comparison of the benefits of onboard versus Thales CipherTrust Manager:

Functionality	Onboard Key Manager	CipherTrust Manager
Broad use cases; Government, Healthcare, Financial, Retail, Legal, Education etc.	Limited	✓
FIPS Compliance (FIPS 140-2) Level 1: Basic. Crypto Algorithm meets approved standards Level 2: Level 1 + Tamper Detection Level 3: Level 2 + Tamper Detection & Response Circuitry	Level 1	Choice of Level 1, 2 and 3
Centralize Key Management - Multi Cluster Reduced complexity for large deployments & distributed infrastructure	✗	✓
Support for Heterogeneous Environments Support multi vendor systems & private, Public or Hybrid cloud	✗	✓
Support for KMIP Standard along with NAE-XML, REST etc. (>45 tested and documented OASIS KMIP product Integrations)	✗	✓
Authentication keys separate from encrypted data	✗	✓
Centralized Audit Logs For all key Mng Actions & entire Key Lifecycle	✗	✓
Separation of duties Separate key ownership and management based on roles and responsibilities to help protect against conflict of interest.	✗	✓
High-Availability Built in Redundancies	✗	✓

Thales CipherTrust Manager is available in the following physical and virtual form factors. Organizations benefit from its flexible options for secure and centralized key management - deployed in physical, virtualized infrastructure, and public cloud environments.

Thales CipherTrust Manager

Features	Physical Appliances	Virtual Appliances
Max keys	1,000,000	25,000
Max concurrent clients per cluster	1,000	100
FIPS 140-2 Support*	L2 L3 with an external or built-in HSM	L1 L3 with an external HSM
Supports the Thales Data Protection Portfolio	Yes	Yes
Redundant hot-swap HDs & Power	Yes	N/A

Learn More

Visit us at https://cpl.thalesgroup.com/ to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

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

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us