

NetApp and Thales CipherTrust Manager Cost-Effective Key Management for Physical and Virtual Environments



The Challenge

Securing Sensitive Data

The need to protect sensitive data has never been greater. Organizations continue to migrate to virtual data centers and cloud environments while dealing with the persistent threat of data breaches. Regulatory demands (e.g. PCI/DSS, HIPAA/HITECH, GDPR, GLBA, and SOX) continue to proliferate. To guard against unauthorized use, many organizations now rely on encryption to protect their data. Creating, managing and safeguarding multiple encryption keys from a centralized location is an essential and crucial part of the process. Strong encryption is vital but it is even more critical to ensure that keys are safeguarded properly with the proper audit control in place.

Together, Thales and NetApp provide an enterprise key management solution with centralized key management, key storage and audit control for both the physical and virtual environments. Depending on FIPS level certification and performance requirements, customers can opt for either a physical appliance or a hardened software (virtual appliance) that runs as a virtual machine (VM) on a server that they already own.

The Solution

Flexible, secure key management

Partnering with Thales, NetApp offers a comprehensive storage security portfolio that delivers encryption flexibility, increases efficiencies, and reduces risk of theft or unauthorized access to stored information. Organizations benefit from a network storage environment that delivers the unique features of the clustered Data ONTAP® operating system combined with Thales CipherTrust Manager Enterprise key management to make sure that encrypted data remains available at all times for your users and important workloads

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

The CipherTrust Manager additionally enhances key management by providing convenient back-up services and delivering strong separation of duties for increased security. The 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.

Hardened Virtual Appliance

Thales CipherTrust Manager includes features that provide hardened security, eliminating many risks and threats to sensitive data. These features include:

- Centralized key management and encryption for virtual environments
- Hardened OS and complete virtual appliance encryption for enhanced key security and protection against snapshot attacks
- Integrated when needed with external HSM to meet higher level compliance standards such as FIPS 140-2, Level 3, PCI-DSS etc
- Accelerated deployments

Proven Key Management

Thales is the largest company exclusively focused on the protection of high-value information assets, with an extensive portfolio of solutions that enable security teams to centrally employ defense-in-depth strategies.

- Enterprise key management leader
- High availability to support cloud-scale deployments
- Proven performance profile
- Central management of multiple key types: symmetric, asymmetric, secret data, and X.509 certificates

Thales offers customers the flexibility of physical or virtual appliances to meet their business needs. Thales is one of the only solutions provider that offers a virtual key management appliance integrated with hardware root of trust that can be used in the public cloud.

Cost Efficient

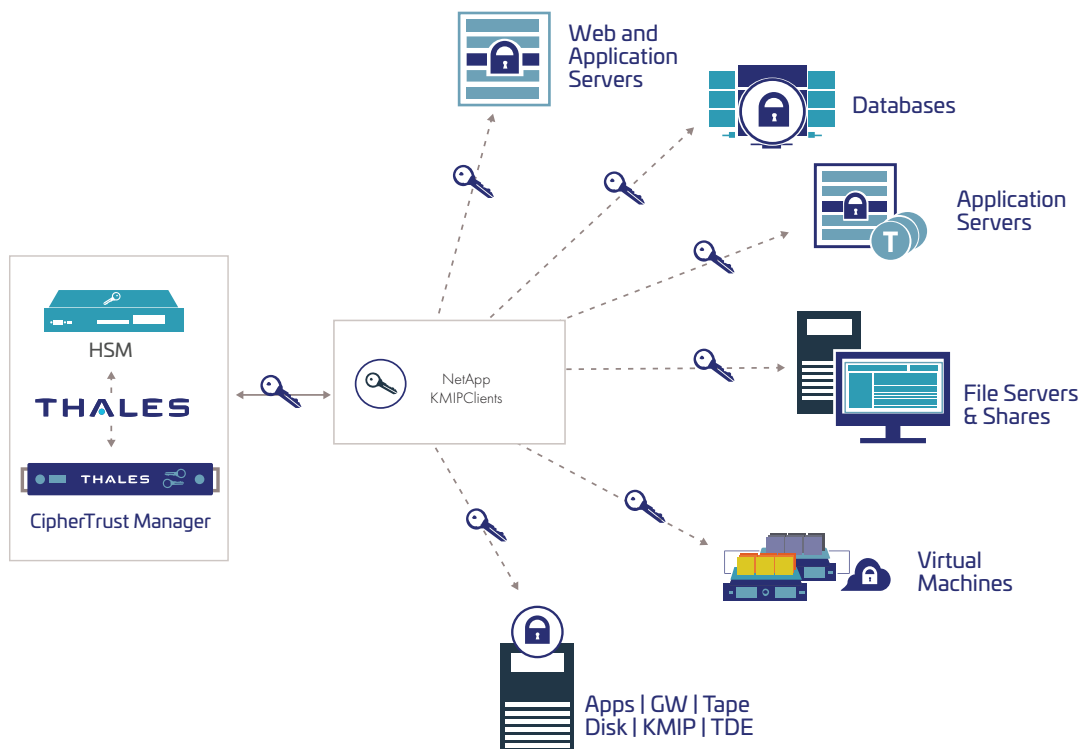
Thales CipherTrust Manager fits many budgets:

- CipherTrust Manager runs as a VM on customers own server and thereby eliminates the need for an additional space.
- Support for the OASIS KMIP standard enables increased centralization of encryption key management over time.
- Well suited for opex models as it eliminates the need for upfront payment.

Standards Compatible

Thales CipherTrust Manager supports KMIP, allowing customers to consolidate key security policies and protect investments across disparate encryption systems, self-encrypting drives, tape archives, storage area networks, virtual workloads, and more.

- **HSM Integration for Secure Deployments:** Thales CipherTrust Manager can reference a master key resident on the HSM as a root of trust for all keys created in the customer's environment. CipherTrust Manager supports Amazon Web Services CloudHSM for subscription-based AWS environments, and SafeNet Luna SA for on-premises deployments
- **Securing Physical and Virtual Storage Environments:** Supports many popular NAS, tape, and backup storage devices from NetApp, IBM, Hitachi Data Systems, Dell EMC, Quantum, HPE, Nutanix, VMware vSAN, and others.
- **Support for Multiple Private/Public Clouds:** Thales CipherTrust Manager can support multiple private and public cloud environment: AWS, VMware (including Public Clouds which support VMware), OpenStack, Microsoft Azure, Microsoft Hyper-V, Google, and others.



Key Benefits

Full Lifecycle Key Support

- Automated, policy-driven operations simplify key management across the entire lifecycle, including secure key generation; storage and backup; and key distribution, deactivation, and deletion.

Unified Key Management

- Centralized administration defines granular access, authorization controls, and separation of administrator duties across multiple encryption deployments.

Intelligent Key Sharing

- Deployed in flexible, high-availability configurations across geographically dispersed centers or service provider environments.

Audit Trail

- Centralized management includes detailed logging and audit tracking of all key state changes, administrator access, and policy changes.

Thales CipherTrust Manager for NetApp ONTAP

Thales CipherTrust Manager maintains data confidentiality on Thales CipherTrust Manager for NetApp ONTAP through efficient centralized key management, and enforcing customized security policies surrounding data access. This combination of a modern storage infrastructure and SafeNet key management delivers the peace of mind that your data and its encryption keys are protected against unauthorized access, while simultaneously making the most efficient use of your storage investments. With SafeNet KeySecure, administrators can simultaneously manage keys associated with NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) starting in ONTAP 9.3, Thales's CipherTrust Data Protection portfolio, and other KMIP-based encryption solutions.

Supporting a Broad Ecosystem

Thales CipherTrust Manager is the industry's leading platform for the centralized management and security of encryption keys. Encompassing Thales and third-party products, Thales CipherTrust Manager supports a broad encryption ecosystem for the protection of sensitive data in storage, virtual workloads, and applications across traditional and virtualized data centers and public cloud environments.

About NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. For more information, visit www.netapp.com. #DataDriven

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.