NetApp and Thales Deliver a Cost-Effective Centralized Key Management Solution

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 (EKM) to make sure that encrypted data remains available at all times for your users and important workloads

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.

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

The 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, k170v, is FIPS 140-2 level 1 compliant.

Key Benefits of an Integrated Solution

- Centralized key management of encryption keys
- Centralized and simplified key management for your entire NetApp infrastructure while improving compliance and auditability.
- Enable multi-tenant data isolation and leverage shared resources while securing data by business policy to segregate data for multiple departments, business units, or customers.
- Achieve high-availability to support cloud-scale deployments
- Ability to cluster multiple Thales CipherTrust Manager appliances to maintain encrypted data availability even in geographically dispersed data centers.
- Enable auditing, logging, and alerting
- Improve regulatory compliance for your entire NetApp environment with a non-repudiative audit trail.

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 CipherTrust Manager 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.

Benefits of Thales CipherTrust Manager in NetApp Storage Environments

- Maximized security. Thales CipherTrust Manager centralizes all key management activities, including key signing, role based administration, quorum control, and the backup and distribution of encryption keys. For sensitive security operations, you can stipulate multiple credential authorization from multiple administrators.
- Resiliency and high-availability. Multiple CipherTrust Manager appliances can be clustered for high-availability with configuration information replicated

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 virtual appliance 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 virtual appliance supports Amazon Web Services CloudHSM for subscription-based AWS environments, and Thales 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 virtual appliance can support multiple private and public cloud environments: AWS, VMware (including Public Clouds which support VMware), OpenStack, Microsoft Azure, Microsoft Hyper-V, Google, and others.

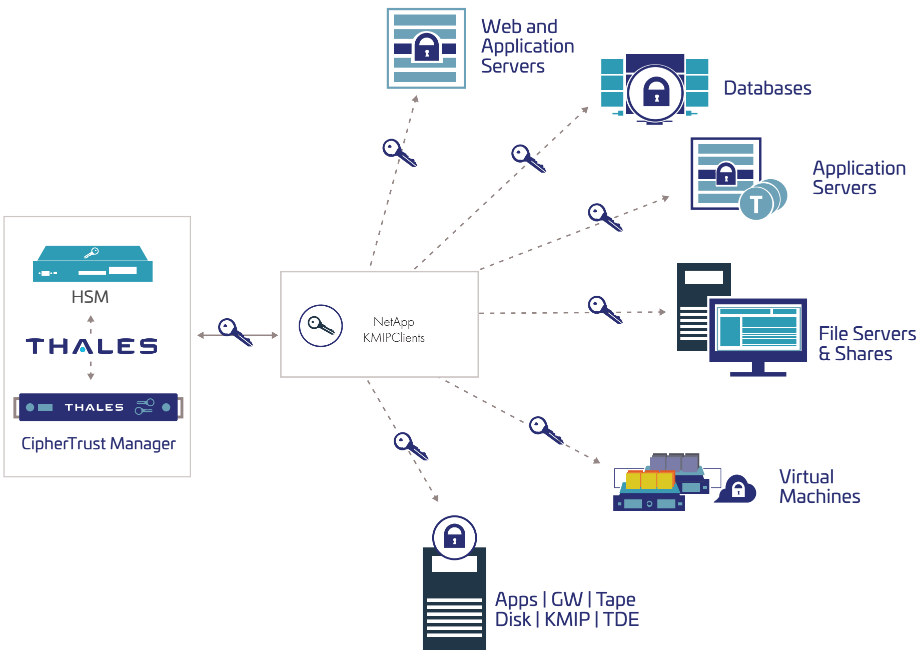

Figure 1: Application data protection and centralized key management across stored data, archive data, virtual workloads.

Key Benefits

Full Lifecycle Key Support

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

- The solutions 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 NetApp Cloud ONTAP through efficient centralized key management, and enforcing customized security policies surrounding data access. This combination of a modern storage infrastructure and Thales 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 Thales CipherTrust Manager, administrators can simultaneously manage keys associated with NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) starting with ONTAP 9.3 and above, Thales.

Supporting a Broad Ecosystem

Thales CipherTrust Manager is the industry's leading appliance for the centralized management and security of encryption keys. Encompassing Thales and third-party products, Thales CipherTrust Manager supports a broad encryption ecosystems for the protection of sensitive data in storage, and 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.

CipherTrust Manager Purchasing Options

	CipherTrust Manager		
	Option I:	**Option II:**	**Option III:**
Purchase Option	Virtual Appliance (runs as VM oncustomer provided server)	Dedicated Appliance without Hardware Security Module (HSM)	Dedicated Appliance with Hardware Security Module (HSM)
Type of Key Storage	Hardened Software	Hardware-based	Hardware-based
Option to add Hardware-based key vaulting via external HSM	Yes	Yes	N/A, as HSM is built-in
FIPS 140-2 Certificate Level	Level 1	Level 1 and 2	Level 1, 2 and 3
	• Crypto algorithm meets approved standards • Able to support Level 2 and 3 with an external HSM	• Adds tamper detection evidence on hardware (e.g. a broken seal on the appliance) • Able to support Level 3 - with an external HSM	• Adds tamper detection and response circuitry • Meets more stringent compliance standards such as PCI-DSS
Thales Product Offering (example)	CipherTrust Manager K170V	CipherTrust Manager - K470	CipherTrust Manager - K570

> cpl.thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: apacsales.cpl@thalesgroup.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com