cpl.thalesgroup.com

THALES
Building a future we can all trust

Enterprise Key Management for Storage Infrastructure

Security conscious organizations are adopting Key Management Interoperability Protocol (KMIP) compliant integrations of their existing storage infrastructure with Enterprise Key Management (EKM) systems. KMIP simplifies the requirement of separating keys from encrypted data, and allows those keys to be centrally managed with a common set of policies from a corporate perspective. Thales offers CipherTrust Manager as the central enterprise key management solution for an expansive ecosystem of storage and archive infrastructure vendors.

Overview

Encryption is fundamental to any defense-in-depth strategy whether the goal is compliance or securing sensitive data. Purpose built or software defined storage solutions are an effective way to deploy encryption (using either self encrypting drives or controller based) in large-scale storage environments. However, as the number of drives or storage end points increase, so does the complexity with increasing number of encryption keys, key stores, and access policies needing management. To cost-effectively support such an environment and bring it into regulatory compliance, enterprise key management must be part of a secure solution.

Solution

Thales' CipherTrust Manager integrates with a multitude of storage products to provide robust, enterprise-scale key management, ensuring that access keys are managed throughout their lifecycle and properly secured with FIPS 140-2 certified internal or external Hardware Security Module (HSM). CipherTrust Manager is also available as a virtual appliance providing organizations with a scalable less expensive alternative to using a physical appliance.

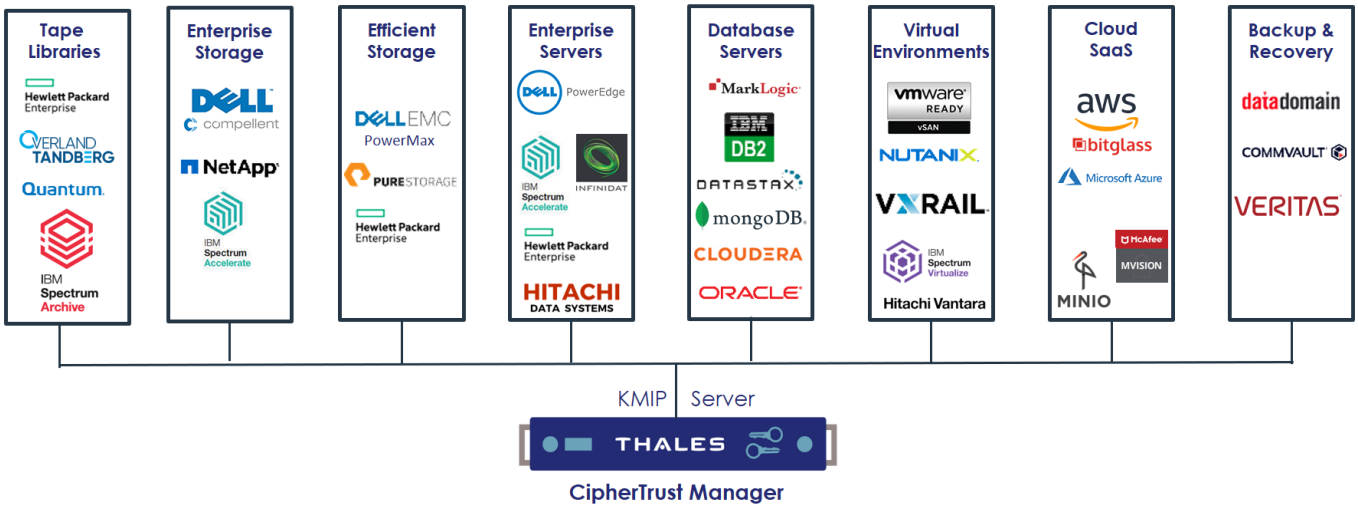
CipherTrust Manager Integrates with Various Storage Solutions

CipherTrust Manager is pre-integrated with a variety of storage and archive solutions via the Key Management Interoperability Protocol (KMIP) to centrally manage key life-cycle for encrypting/decrypting data. Consolidating the policy and key management of servers, databases, and file storage streamlines security administration. Centralized key management improves security by making key creation, rotation, and deletion easier, while also separating duties so that no single administrator is responsible for the entire environment. Additionally, unifying and centralizing policy management, logging, and auditing makes information more readily accessible which, in turn, makes demonstrating compliance with data governance requirements simple.

Virtual CipherTrust Manager allows organizations to utilize a secure virtual appliance to centrally manage encryption keys and enforce access control across cloud infrastructures. It also ensures that organizations maintain ownership of their encryption keys at all times by hardening the appliance OS and encrypting the entire virtual appliance for enhanced key security and protection against snapshot attacks. CipherTrust Manager provides scalable key management and secure encryption at remote facilities or cloud infrastructures.

Summary of Benefits:

Thales' CipherTrust Manager provides customers with complete control by securing the keys needed to access the storage system. Together, Thales and their storage partners offer a secure and efficient means of protecting data at rest with encryption, and help customers meet data security compliance mandates such as FIPS 140-2, PCIDSS, HIPAA, and GDPR.



Centralized Management of Access Keys

Centralize and simplify key life-cycle management (e.g. key generation, rotation, etc.) for various storage platforms and KMIP-compatible encryption solutions, while improving compliance and auditability.

High-Availability Configurations

Cluster multiple CipherTrust Manager appliances to maintain encrypted data availability, even in geographically dispersed data centers.

Hardware or Software Appliance

CipherTrust Manager is available in both physical and virtual form factors. By utilizing CipherTrust Manager, organizations benefit from its flexible options for secure and centralized key management – deployed in physical, virtualized infrastructure, and public cloud environments.

Separation of Duties

CipherTrust Manager supports segmented key ownership and management based on individuals or group owners. This approach is perfect for dividing large enterprises into multiple administrative domains based on organizational structure.

Ecosystem Support

When there are dispersed data repositories with varying security concerns among lines of businesses consuming these repositories, CipherTrust Manager enables businesses to bring all these disparate efforts under one umbrella from a policy management viewpoint. The CipherTrust Manager EKM solutions including the KMIP technology standard help in providing a consistent interface to applications and appliances interfacing with the external key management system.

Conclusion—Secure the Breach

Encrypting data in the storage environment is critical to ensuring that data is safe in the event of a data breach. Thales has partnered with a number of storage vendors to offer organizations the ability to secure data through encryption without making the management of the necessary encryption keys and policies unwieldy or difficult.

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.

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