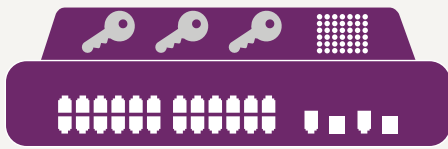


SOLUTION BRIEF



# Benefits of Enterprise Key Management for Storage

The storage market is seeing an increase in KMIP (Key Management Interoperability Protocol) compliant Enterprise Key Management (EKM) integrations from storage vendors. Security-conscious organizations are driving these integration requests due to the multitude of benefits that an EKM, like SafeNet KeySecure can provide an organization with. Gemalto has an expansive ecosystem of partners that offer storage and archive products that integrate with SafeNet KeySecure to provide organizations with powerful encryption and key management solutions.

## 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 do the 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 the solution.

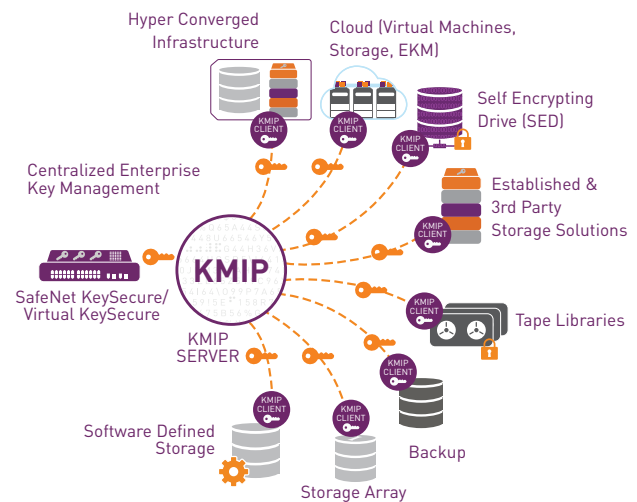
## Solution

Gemalto's SafeNet KeySecure 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 hardware. Gemalto also offers a hardened virtual security appliance that provides organizations with a more operational—and expense friendly alternative to using a hardware appliance.

## Gemalto's SafeNet KeySecure and SafeNet Virtual KeySecure Integrates with Various Storage Solutions

Gemalto's SafeNet KeySecure is a key management appliance that integrates with a variety of storage and archive solutions via the Key Management Interoperability Protocol (KMIP) to store and centralize the management of the Authority Credentials. Consolidating the policy and key management of servers, databases, and file storage streamlines security administration. Centralized key management improves security by making key surveillance, 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. Gemalto's SafeNet Virtual KeySecure allows organizations to utilize a secure virtual appliance to manage keys as well as data encryption, 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. SafeNet Virtual KeySecure provides scalable key management and secure encryption at remote facilities or cloud infrastructures. By using a virtual key manager instead of a hardware appliance, organizations can scale key management in private or public cloud infrastructures, and eliminate the cost for additional rack space.



SafeNet KeySecure provides organizations using various storage endpoints with a secure, enterprise key management solution. The Key Management Interoperability Protocol (KMIP) is a specification developed by OASIS that standardizes communication between enterprise key management systems and storage/encryption systems.

## Summary of Benefits:

Gemalto's SafeNet KeySecure provides customers with complete control by securing the keys needed to access the storage system. Together, Gemalto 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 management (e.g., escrow, recovery) for various storage platforms and KMIP-compatible encryption solutions, while improving compliance and auditability.

## High-Availability Configurations

Cluster multiple SafeNet KeySecure appliances to maintain encrypted data availability, even in geographically dispersed data centers.

## Hardware or Software Appliance

SafeNet KeySecure is available as a hardware appliance or hardened virtual security appliance. By utilizing SafeNet KeySecure, organizations benefit from its flexible options for secure and centralized key management – deployed in physical, virtualized infrastructure, and public cloud environments.

## Separation of Duties

SafeNet KeySecure supports segmented key ownership and management based on individuals or group owners. This approach is perfect for protecting sensitive material against unauthorized access from staff.

## Ecosystem Support

Sometimes, it's difficult to envision how much effort is involved when it comes to managing your sensitive data and where it exists. Databases, CRM/ERP systems, various commercial and in-house applications are among the few places where the proper management of sensitive data needs to be considered. Where there are more dispersed data repositories (as well as different security concerns among lines of business consuming these repositories), SafeNet KeySecure helps bring all this disparate effort under one umbrella from a policy management viewpoint. An EKM like SafeNet KeySecure that includes technology standards such as KMIP helps provide a consistent interface to applications and appliances interfacing with the external key management system.

Gemalto has an expansive ecosystem of partners that offer storage and archive products that integrate with SafeNet KeySecure to provide organizations with powerful encryption and key management solutions, including:

DELL EMC

vmware®

NUTANIX

NetApp®

CISCO™

Hewlett Packard Enterprise

HUAWEI

IBM

Tintri



COMMVault™

Quantum®

Hitachi Data Systems

## Conclusion—Secure the Breach

Encrypting data in the storage environment is critical to ensuring that data is safe in the event of a security breach. Gemalto 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.

**Contact Us:** For all office locations and contact information, please visit [safenet.gemalto.com/contact-us](https://safenet.gemalto.com/contact-us)

**Follow Us:** [blog.gemalto.com/security](https://blog.gemalto.com/security)

 [GEMALTO.COM](https://GEMALTO.COM)

**gemalto**  
security to be free