SafeNet

THE DATA PROTECTION COMPANY

Protecting Quantum Tape Libraries with SafeNet KeySecure

SOLUTION BRIEF

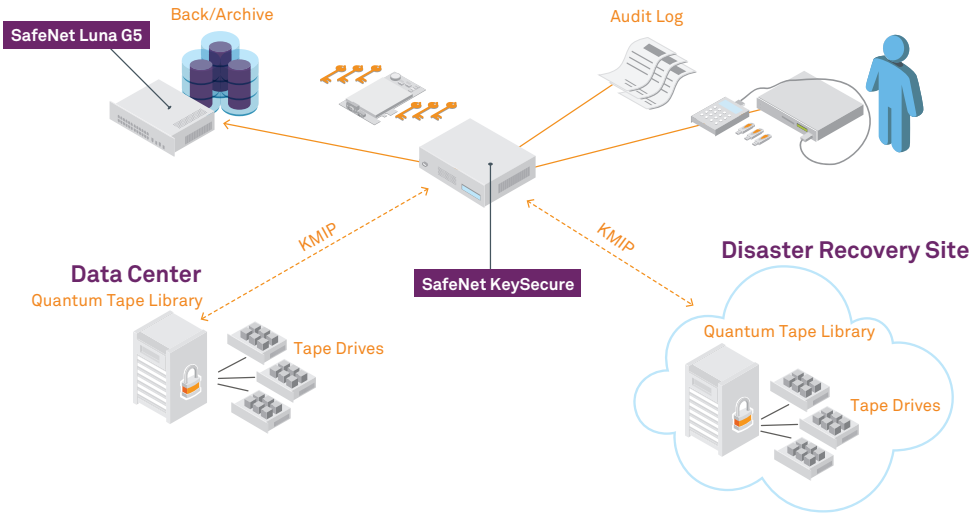
Benefits

- Unified key management platform with centralized key lifecycle management
- Manages heterogeneous encryption keys and key materials
- KMIP Standards-based Interoperability
- Granluar Policy management on keys and user
- High assurance and reliability

Explosive data growth, accelerating trends in virtualization and multi-tenancy, increased sophistication of data breaches, and more stringent government regulations are challenging enterprises to securely retain and archive data. Additionally, the need to store data for longer periods of time to meet business best practices - often triggered from compliance mandates and theft prevention while maintaining business continuity for authorized user access to the data - is only adding to these challenges. To solve these concerns, enterprises are deploying a combination of storage security solutions, such as storage encryption, encrypted tape libraries, and self-encrypting tape drives. When encryption is being used for the protection of important data, such as high trust assurance, data integrity, adequate access policies, and proper utilization of encryption, key management is an essential element in the equation. A common practice today relies on vendor-specific key management leading to fragmented key stores that need to be managed and maintained individually. For global enterprises, this leads to increased data risks as key lifecycle management occurs regionally and not centrally.

As the use of tape libraries proliferates throughout an organization, enterprises must scale the lifecycle management of encryption keys, including key generation, import/export, distribution, rotation, and destruction. Having the capability to centrally manage and enforce tape drive encryption keys and associated policies for regional, virtual, and cloud-based tape libraries provides an effective control to eliminate fragmented key stores, lost and stolen keys, and unauthorized access to business critical information.

SafeNet KeySecure is a robust enterprise key lifecycle management solution, with the ability to consolidate and centrally manage encryption keys from multiple tape libraries and disparate encryption platforms. KeySecure communicates with tape libraries (such as Quantum tape libraries) for the purpose of key management through KMIP, an OASIS interoperability protocol. KMIP enables enterprises to standardize on a strong interoperability protocol for communication.



Features

- Key Vault
- Secure Key Sharing, Backup, and Recovery
- Non-Repudiative Key Lifecycle Management
- Key Destruction or Invalidation
- High Assurance and Availability

Tape drives/tape cartridges attach to tape libraries—each with their own key management solution. These drives may be self-encrypting LT04 & LT05 drives. When a new tape drive/cartridge is added or changed, the tape drive requests a key from the tape library which, in return, requests the key from KeySecure. KeySecure generates the key with defined key attributes and sends it back to the tape library which, in turn, sends the key identifier to the tape drive/tape cartridge. Tape drives/tape cartridges store the key identifier. The master key is stored within the hardened boundary of KeySecure. The tape drive/tape cartridge uses the key to encrypt all the data stored on the tape drive. Interaction between the user and the data is based on the key attributes defined within KeySecure and the associated key. KeySecure records key states and attribute changes, and maintains this information securely in the KeySecure logs.

Every tape drive/tape cartridge has its own unique key. As tape drives are deployed, removed, and repurposed, and data is secured on the tape drive, keys are required, depending on the action; the number of keys can grow exponentially. This may result in thousands of keys. KeySecure is the ideal solution to centrally store, manage, and protect millions of tape library and tape drive keys, while ensuring keys are secure and the data is always available to authorized users.

Centralized Lifecycle Key Management

KeySecure can centrally manage crypto keys and passwords for Quantum tape libraries and their associated tape drives/tape cartridges to preserve and safeguard persistent data stored to meet data retention laws, compliance mandates, and contingency planning requirements. KeySecure will consolidate and securely archive all cryptographic keys while maintaining a non-repudiative key lifecycle management log for auditors. By centralizing key lifecycle management, enterprises can easily validate and verify any key state and key attribute changes for all tape libraries and associated tape drives.

Based on Open Standards

SafeNet's KeySecure, with its conformance to the OASIS KMIP specification and in combination with Quantum's KMIP-compliant tape libraries, enables enterprises to manage cryptographic modules and KMIP-compliant tape libraries within a single centralized management system. Quantum tape libraries protect the data at rest with the help of KeySecure since it manages the cryptographic keys and user access policies to the data.

Granular Policy Management

KeySecure protects the data through separation of duties based on unique key identifiers. This is defined by individual or group-level authorization in conjunction with defined key validity timeframes. In instances of multi-tenant environments, or on devices where information is stored or shared between groups, departments, partners, and customers, the granular key administration allows for the co-mingling of data without compromising or exposing data. By enforcing granular policy management based on the user and associated key identifier, enterprises are keenly aware of any unauthorized data access or potential data breach.

Assuring Compliance

KeySecure provides a detailed audit trail of key usage and data access, mostly required by regulatory mandates. To assure audit trail authenticity, KeySecure also provides cryptographic assurance that key logs are authentic. Each log is digitally signed, recorded, and stored by KeySecure. A secure and verifiable audit trail is critical for ensuring that key requests and key state changes are authentic, including administration functions and operational messages.

Key Management Features

Key Vault: KeySecure ensures that key policies are defined and managed from a central location. Keys are generated, securely hosted on KeySecure, and distributed to the tape library, and then to the tape drives/tape cartridges to encrypt or decrypt the data. KeySecure consolidates and centralizes key lifecycle management across millions of tape library/tape drive encryption keys.

Secure Key Sharing, Backup, and Recovery: KeySecure centrally manages, maintains, and synchronizes all keys and their attributes, ensuring data access in the event of infrastructure and product failures, and disaster recovery and backup. Keys are retrieved based on unique identifiers, securely passed from the Quantum tape libraries to the key management console. Using KeySecure, security administrators can seamlessly archive and restore all applicable keys and key attributes for Quantum tape libraries and tape drives. For tape drives restored back into the infrastructure, KeySecure will securely provide the key for data retrieval.

Non-Repudiative Key Lifecycle Management: As keys age or business policy dictates, keys are versioned on KeySecure and distributed to the tape library and associated tape drive/tape cartirdge. KeySecure maintains all key state changes based on defined business policies and logs all key state changes.

Key Destruction or Invalidation: With centralized key management, tape destruction or invalidation is easily achieved when the encryption key on KeySecure is destroyed. Role-based administration functions can be defined to distribute responsibility and control across multiple individuals—a single individual is unable to access, copy, or destroy data.

High Assurance and Availability: Due to the nature of the solution, KeySecure—a hardened, hardware solution—easily assimilates into your existing infrastructure and scales as needed. It can seamlessly manage millions of keys and their data access policies, regardless of the sophistication of the deployment. Enterprises can compartmentalize data on tape libraries and restrict user access based on key identifiers or defined key groups. Users will only be able to access data on defined devices based on defined policies, allowing data to co-mingle without the concern of unauthorized access. As devices or keys are moved, user access controls are also moved or may be redefined.

SafeNet KeySecure: Enterprise Key Management

KeySecure simplifies lifecycle key management, making it efficient for security teams to consolidate data security over time and across the enterprise. With KeySecure, administrators can create hierarchical key-sharing groups that enable fast, efficient key management across multiple organizations—while ensuring relevant policies for different groups are consistently enforced. Centralized enterprise key and policy management enables compliance, and ensures stronger data use and tracking control. KeySecure provides a secure repository for all sensitive crypto objects, including symmetric and asymmetric keys and certificates. KeySecure can assign and perform key lifecycle policies for all Quantum tape libraries.

About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies, and in over 100 countries, trust their information security needs to SafeNet. For more information, visit www.safenet-inc.com.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected