



Honey, Where Are My Keys?

SafeNet KeySecure - Enterprise Key Management

CUSTOMER VALUE PROPOSITION

SafeNet KeySecure is an Enterprise Key Management (EKM) solution that enables a single, centralized solution for managing cryptographic keys and applications. As the use of encryption proliferates throughout the corporation, security teams must scale their management of encryption keys, including key generation, key import and export, key rotation, and much more. With KeySecure, administrators can simultaneously manage multiple, disparate encryption appliances and associated keys through a single, centralized key management solution.

CUSTOMER BUSINESS CHALLENGES

- Implementing encryption is fundamental for solving compliance mandates and as an info-security risk mitigation tool.
- Companies view encryption as a commodity – a necessary process to manage risks, ease proof of compliance, and ensure the protection of data.
- Security teams struggle with the administrative efforts of managing encryption deployments and associated key lifecycle operations.

USE CASES

- Centralize key administration to create, maintain, protect, and control the use of cryptographic keys through their lifecycle
- Centralize management of de-centralized HSMs
- Granular key administration for storage and backup/archive applications
- Secure key management and storage of virtual security applications

KEYSECURE FEATURES AND BENEFITS

- Consolidates and centrally manages a wide variety of key management protocols, applications and encryption utilities.
- Supports KMIP and standard management protocols from legacy devices
- Consolidates key security policies across multiple disparate encryption systems
- Easily manages and protects keys for physical, virtual, and cloud-based data – preventing data exposure to administrators (cloud and on premise), lawful surrender based on server co-residence, and unauthorized data copying and destruction
- Granular authorization controls based on user key permissions
- Centrally manage geographically dispersed encryption deployments
- Enable uniform, consistent policy management across heterogeneous encryption deployments
 - Verifiable audit trail for all key management actions
 - Separation of duties through individual or group-level authorization
- Agnostic to the IT infrastructure—physical, virtual, and cloud form factors addressed
- Agnostic to the scale of the organization—scales as the enterprise grows and/or evolves
- Tamper-proof, hardware-based platform with FIPS 140-2 Level 3 assurance (validation in process)

TARGET CUSTOMER PROFILE

KeySecure enterprise key management prospects are:

- Existing NetApp DataFort customers
- Large-scale Luna HSM customers
- NAS, SAN & DAS storage customers
- Brocade BES storage customers
- Quantum Tape Libraries customers
- KMIP-compliant clients

CONVERSATION STARTERS AND QUALIFICATION QUESTIONS:

- Do you use storage encryption to protect your data?
- Do you use backup/archive encryption?
- How are you managing the keys that protect your cloud or shared data?
- How do you provide key lifecycle management (key rollover, key versioning, policy management) for your encryption keys?
- Would centralizing key rotation, key revocation, and key maintenance benefit your organization?
- How are you validating compliance for your encryption keys (auditing, logging, and alerting on key state changes)?
- How are you managing the keys that protect your cloud or shared data?

COMPETITION AND KEY DIFFERENTIATORS

Competitors: IBM Tivoli Key Lifecycle Manager, RSA Data Protection Manager (formerly Key Manager)

Key Differentiators:

- Heterogeneous solution offering
 - Storage encryption products
 - NAS, SAN, DAS and archive
 - NSE/FDE self-encrypting drives
 - Hardware security modules
 - SafeNet ecosystem products
 - Third-party integration with KMIP-compliant clients
 - Quantum Tape Libraries
- Easy-to-use, self-contained, hardened hardware/appliance-based solution
- SafeNet’s strong market penetration
- SafeNet’s institutional and accumulated knowledge of enterprise encryption

CALL TO ACTION

How does the NetApp Partnership effect how you sell or what you can sell?

If a deal touches NetApp products, or NetApp brings SafeNet into a deal, we need to execute the deal through NetApp or as directed by NetApp, or through their assigned channel partner.

Email netapp-sales@safenet-inc.com to demonstrate the product or offer an evaluation unit.

PRODUCT OPTIONS AND FEATURES

	KeySecure k460	KeySecure k150
Max keys (symmetric & asymmetric keys stored per cluster)	1,000,000	25,000
Max concurrent clients	1,000	100
Redundant, hot-swappable hard drives & fans	Yes	No
Scalability	unlimited	unlimited
FIPS 140-2 level 3	Embedded LUNA K6 card (in process)	No
Supported Appliances		
KMIP compliant	Yes	Yes
Cloud Encryption/Virtual	Cloud Enabled ProtectV (Q2 2012)	Cloud Enabled ProtectV (Q2 2012)
Tape Libraries	Quantum Tape Libraries	Quantum Tape Libraries
NAS, SAN, self-encrypting storage appliances	SafeNet StorageSecure (Q1 2012) NetApp DataFort and LKM NetApp NSE Brocade SAN Encryption Switch (BES)	NetApp NSE
Hardware Security Modules (HSM)	SafeNet LUNA SA (Q1 2012) SafeNet LUNA PCI (Q1 2012)	

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

Follow Us: www.safenet-inc.com/connected

©2011 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. BC (EN)-10.04.11