

SafeNet KeySecure™

PRODUCT BRIEF

SafeNet KeySecure Benefits

- Lower Administration Costs.**
Lowers the costs of encryption and key management with centralized administration and automated operations
- Simplified Compliance.**
Centralized, efficient auditing of key management practices saves staff time and decreases the time spent on compliance mandates
- Lower Total Cost of Ownership.**
Low TCO for key management deployments leveraging a large and growing list of encryption products with the OASIS KIMP standard ensures KeySecure can address future key management needs
- Security and Compliance for Cloud Environments.**
Take advantage of the lower costs of virtualized and cloud environments with flexible deployment options and appliance models covering physical, virtualized (VMware) and public cloud (AWS Marketplace) environments
- Risk Mitigation with Maximum Key Security.** Tamper-proof hardware options and hardened virtual appliance supporting a hardware root of trust with SafeNet's Luna HSM or using Amazon's CloudHSM service

Overview

SafeNet KeySecure is the industry's leading platform for the centralized management and security of encryption keys supporting a broad encryption eco-system—encompassing SafeNet and third-party products—for the protection sensitive data in storage, virtual workloads and applications across traditional and virtualized data centers and public cloud environments.

Only SafeNet delivers enterprise key management in flexible deployment options spanning FIPS 140-2 Level 3 or 2 validated hardware appliances and hardened virtual appliances supporting a hardware root of trust using SafeNet Luna Hardware Security Modules (HSM) or the Amazon CloudHSM service.

Highlighted Capabilities

- Heterogeneous Key Management.** Manages keys for a variety of encryption products including self-encrypting drives, tape archives, Storage Area Networks, virtual workloads, applications and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.
- Multiple Key Types.** Centrally manages symmetric, asymmetric, secret data, and X.509 certificates along with their associated policies.
- Full Lifecycle Key Support and Automated Operations.** Simplifies the management of encryption keys across the entire lifecycle including secure key generation, storage and backup, key distribution and key deactivation and deletion. KeySecure makes automated, policy driven operations easy for tasks such as key expiry and key rotation.
- Centralized Administration of Granular Access, Authorization Controls and Separation of Duties.** Management console unifies key management operations across multiple encryption deployments and products while ensuring administrators are restricted roles defined for their scope of responsibilities.
- High-Availability and Intelligent Key Sharing.** Deploys in flexible high-availability configurations within an operations center and across geographically dispersed centers or service provider environments using an active-active mode of clustering.
- Auditing and Logging.** Centralized management includes detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation.
- Next-Generation Solution for NetApp Storage.** The official upgrade for existing NetApp DataFort Encryption Appliance and NetApp Storage Encryption deployed with the NetApp Lifetime Key Manager.

Supported Technologies (All Models):

API Support

- KMIP 1.1, PKCS #11, JCE, MS-CAPI, and .NET

Network Management

- SNMP (v1, v2, and v3), NTP, URL health check, signed secure logs & syslog, automatic log rotation, secured encrypt and integrity checked backups and upgrades, extensive statistics

Appliance Administration

- Secure Web-based GUI, Secure Shell (SSH), and console

Authentication

- LDAP and Active Directory

Hardware Specifications:

KeySecure k460

- Intel Xeon E5620 2.4Ghz processor
- Four (4) 10/100/1000 Mbps Ethernet ports
- Two 500GB 7.2K RPM SATA 2.5"
- 1U, rack mountable (H: 1.7"; W: 19"; D: 30")
- Two 502W Energy Smart power supplies

KeySecure k150

- VIA C3 800MHz processor
- One (1) 10/100 Mbps Ethernet port
- 250W, 100 - 240 VAC, auto-ranging, 50-60 Hz, 5 - 3A power supply
- 1U, rack mountable (H: 1.7"; W: 19"; D: 13")

SafeNet KeySecure k460 and k150

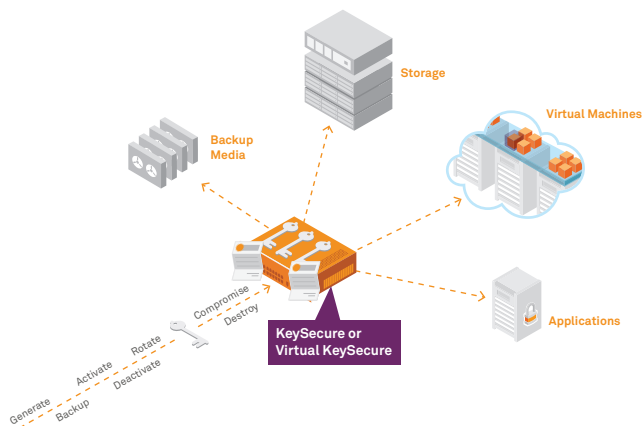
SafeNet KeySecure hardware appliances provide the highest levels of key security and compliance in FIPS 140-2 validated appliances. SafeNet KeySecure k460 delivers robust capabilities including an embedded SafeNet Luna PCI FIPS 140-2 Level 3 cryptographic module. SafeNet KeySecure k150 is a FIPS 140-2 Level 2 validated.

Virtual KeySecure k150v

SafeNet Virtual KeySecure, a hardened virtual security appliance, provides security and centralized management of encryption keys used for the protection of sensitive data in virtualized and cloud environments. With Virtual KeySecure organizations can lower costs and scale key management in cloud infrastructures. With Virtual KeySecure organizations get:

- Centralized key management for virtual environments in a virtual security appliance deployed on VMware (ESXi 4 and ESXi 5) or AWS Marketplace
- Hardened OS and complete virtual appliance encryption for enhanced key security and protection against snapshot attacks
- Hardware root of trust for appliance master key using SafeNet Luna HSM or Amazon's CloudHSM Service
- Accelerated deployments - simply power on the virtual appliance

KeySecure Use Cases



SafeNet KeySecure use cases for centralized key management cover SafeNet and third-party encryption products across storage and archive, virtual workload and application data protection.

SafeNet KeySecure Model Comparison

Feature	KeySecure k460	KeySecure k150	KeySecure k150v
Max keys	1,000,000	25,000	25,000
Max concurrent clients per cluster	1,000	100	100
Redundant hot-swap HDs & Power	Yes	No	N/A
FIPS 140-2 Level 3	Yes (Luna HSM)	No	N/A
Luna HSM Management	SafeNet Luna SA & PCI		
SafeNet ProtectV and ProtectApp	Yes	Yes	Yes
SafeNet StorageSecure	Yes	No	No
Brocade SAN Switch (BES)	Yes	No	No
SafeNet Third-party Integration Support	HP ESL G3, Quantum Scalar Series (i6000, i500 & i40/80), NetApp NSE, Hitachi VSP, Amazon Web Services S3, DropBox, Google Cloud Storage, Google Drive		
Partner Integration Support (requires ProtectApp)	CipherCloud, Persceys, PKZip, Sepaton VTL, ServiceMesh, Viasat		

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

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

©2013 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. PB (EN)-10.22.13