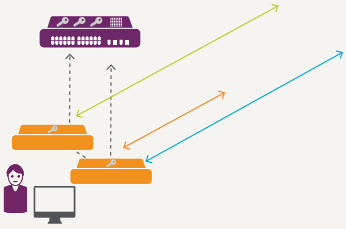


PRODUCT BRIEF

SafeNet Virtual KeySecure

Overview

Organizations rely on encrypting their data as a primary means of protecting it from unauthorized use. An essential part of this process involves creating and managing encryption keys in multiple places, including small- and medium-sized installations and remote locations requiring encryption for data at rest. Many customers are looking for a solution to manage these instances; however, the up-front cost of hardware key management appliances might not fit some budgets.

SafeNet Virtual KeySecure™ is a hardened virtual security appliance that provides organizations with a more operation- and expense friendly alternative to using a hardware appliance for secure key management and meeting security and compliance requirements. By using a virtual key manager instead of a hardware appliance, organizations can scale key management at remote facilities or in cloud infrastructures such as VMware and AWS Marketplace, and eliminate the cost for additional rack space. SafeNet Virtual KeySecure allows organizations to manage keys, unify 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.

Combat Risk and Get Affordable Security

As companies migrate to virtual data centers and cloud environments, sensitive data is likely to reside outside the physical walls of the enterprise, making secure data management a challenge. With regulations such as PCI DSS, HIPAA/HITECH, GDPR, GLBA, and SOX, combined with the high cost of data breaches, the pressure to protect this sensitive data has never been greater.

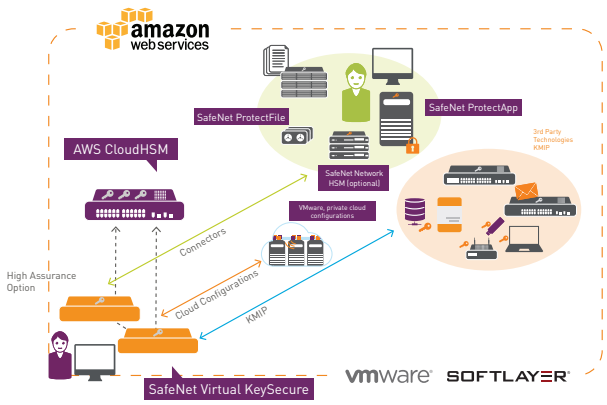
SafeNet Virtual KeySecure provides customers with a virtual appliance that manages and securely stores encryption keys for many different solutions, including SafeNet ProtectV™ virtual machine encryption, NetApp encrypted storage, any KMIP-compliant encryption solution, and many others. Gemalto is the only solutions provider that offers a virtual key management appliance integrated with a hardware root of trust (SafeNet Luna Hardware Security Modules (HSM) or Amazon CloudHSM) that can be employed in the public cloud.

SafeNet Virtual KeySecure Benefits

- SafeNet Virtual KeySecure can be hosted anywhere: on a virtual machine such as VMware or rented from a service- such as AWS Marketplace.
- Support of the SafeNet Data Protection Connector portfolio provides customers with a broad spectrum of use cases that can be supported
- Bring Your Own License (BYOL) for AWS Marketplace enables purchase of the SafeNet Data Protection Connector licenses directly from Gemalto.
- Subscription-based offerings are better suited for operating expenditure (op-ex) models, versus capital expenditure models (standard hardware purchases) that require upfront payment.
- Flexible deployment options can easily scale to provide key management at remote facilities or in cloud infrastructures.
- Compatibility with the OASIS Key Management Interoperability Protocol (KMIP) standard provides support for a large and growing list of encryption products.
- Key security policies can be consolidated across multiple, disparate encryption systems, protecting current investments.
- Centralized, efficient auditing of key management offers simplified compliance for cloud environments and decreases the amount of time spent on compliance mandates.
- SafeNet Virtual KeySecure's hardened virtual appliance mitigates security risks typically associated with software-based implementations.

SafeNet Virtual KeySecure Use Cases

SafeNet Virtual KeySecure provides application data protection and centralized key management for Gemalto and third-party encryption products across stored and archived data, virtual workloads, and application data protection.



Product Highlights:

- **Full Lifecycle Key Support and Automated Operations.** Simplifies management of encryption keys across the entire lifecycle, including secure key generation, storage and backup, and key distribution, deactivation and deletion. SafeNet Virtual 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 that administrator roles are properly defined.
- **High-Availability and Intelligent Key Sharing.** Deploys in flexible, high-availability configurations across geographically dispersed centers or service provider environments.
- **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.

Virtual KeySecure Model Comparison

SafeNet Virtual KeySecure		
Features	**k450v**	**k150v**
Max Keys	1,000,000	25,000
Max concurrent Clients per Cluster	1,000	100
FIPS 140-2 Support	L1	L1
HSM Integration *	Yes	Yes
Supports SafeNet Data Protection Connectors **	SafeNet ProtectApp, SafeNet ProtectDB,SafeNet ProtectFile, SafeNet Tokenization and SafeNet ProtectV	SafeNet ProtectApp, SafeNet ProtectDB,SafeNet ProtectFile, SafeNet Tokenization and SafeNet ProtectV
Supports KMIP	Yes	Yes
CPU	12 CPU (Configurable)	1 CPU Required
RAM	8192 MB (Configurable)	1024 MB Ram Required
Network Adapter	2 (Configurable)	1 Allowed / Available
Gemalto Third-party Integration Support	**Content Management:** Alfresco Open ECM, Open Text (EMC), InfoArchive Stealth Content Store, ServiceNow **Mainframe Encryption:** PKware **Big Data:** Dataguise, DataStax, Hadoop, MongoDB, MariaDB, SAP HANA, Cassandra, Couchbase, Hortonworks, CloudEra **Analytics:** IBM Qradar, HPE ArcSight, Splunk, RSA Security Analytics, Above Security **Application Servers:** IBM WebSphere, Oracle Weblogic, Microsoft IIS, Apache Tomcat, Red Hat JBoss **Backup Solutions:** Commvault Simpana, Symantec NetBackup (via NetApp) Cloud Storage: Nutanix, Amazon Web Services S3, DropBox, Google Cloud Storage, Google Drive, NetApp Cloud ONTAP, NetApp AltaVault, IBM ICDES, Panzura Storage Controller **Cloud Access Security Brokers:** CipherCloud, SkyHigh Networks, Perspecsys (Blue Coat), Hitachi Sepaton VTL, CSC ServiceMesh, Netskope Active Encryption, Vaultive Cloud Data Protection Platform **Databases:** MS SQL Server (EKM), Oracle (TDE), IBM DB2, Oracle MySQL, Oracle Database, Teradata File and Disk Encryption: PKware, IBM, Dell, AWS, Microsoft, LUKS, ViaSat **Identity Management:** Centrify Privilege Service, Lieberman Software **Key Managers:** Hadoop KMS, CloudEra Navigator Key Trustee Server **Physical Storage:** NetApp NSE, Dell Compellent (SC and XC), HPE MSL/ESL Tape Libraries, HPE 3Par StoreServ, HPE XP7, Hitachi, SP, Hitachi HUS, Hitachi RAID700, IBM XIV SED, Quantum Scalar Series(i6000, i500 & i40/80),Viasat, Brocade FS8-18, Huawei Oceanstor, Tintri VMStore, Cisco UCS, SpringPath HyperFlex, NexentaStor 4.5	

*Supports key storage in hardware security modules (HSMs) such as Amazon Web Services CloudHSM in a subscription-based AWS environment, and SafeNet Luna HSM, a hardware appliance option that is deployed on-premises in a range of models and configurations.

**Remote encryption within the SafeNet Virtual KeySecure appliance using the connectors (SafeNet ProtectApp, SafeNet ProtectDB, and SafeNet Tokenization) requires the purchase of SafeNet Crytpo Pack. Local encryption, SafeNet ProtectV and SafeNet ProtectFile do not require SafeNet Crypto Pack feature activation.

Try it before you buy it. Click here to enroll in Amazon Web Services 30-day free trial.

Need an on-premise appliance? Learn more about on-premises enterprise key management.

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

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free