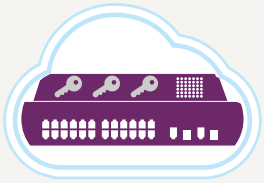
gemalto
security to be free



PRODUCT BRIEF

SafeNet Virtual KeySecure

Overview

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 In private or public cloud infrastructures, and eliminate the cost for additional rack space. 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, the New Generation

Gemalto's latest SafeNet Virtual KeySecure product is the k170v model, which is built on prevailing cloud-based technologies and provides a cloud friendly, key management solution for your organization.

With a REST interface and microservices based architecture, the k170v has been built to easily deploy and scale within your environment. Using the new REST API Playground, developers can explore the new set of key management and administrative endpoints.

Organizations can lower costs and scale key management with a virtual appliance that is quickly deployed for high-availability in various public cloud infrastructures such as Oracle, AWS and Microsoft Azure, or on-premise using Oracle VM VirtualBox VMware vSphere, and Openstack.

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 is a virtual appliance that manages and securely stores encryption keys for diverse encryption solutions,including the SafeNet Data Protection portfolio, traditional storage and hyperconvergence solutions, Big Data, KMIP compliant solutions, 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

Host Anywhere:

- The k150v and k450v models can be rented from a service such as AWS marketplace, or hosted on any virtual environment such as Oracle VM Virtual Box, IBM Marketplace, AWS and others.
- **New!** The SafeNet Virtual KeySecure k170v model provides additional hosting options, and can run as a native virtual machine on VMware, AWS, Microsoft Azure, Oracle VM Virtual Box and OpenStack with more public/private clouds coming soon.

Compatibility:

- Compatibility with the OASIS Key Management Interoperability Protocol (KMIP) standard provides support for a large and growing list of encryption products.
- Support of the SafeNet Data Protection portfolio provides customers with a broad spectrum of use cases that can be supported.
- Bring Your Own License (BYOL) for AWS Marketplace enables purchase directly from Gemalto (available for the k150v and k450v models).

Flexibility:

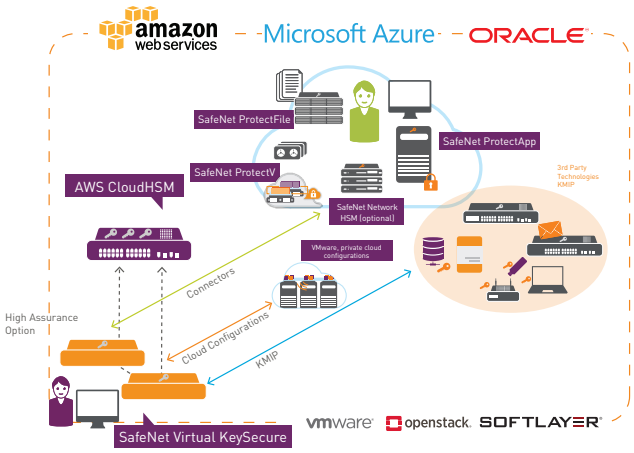
- Subscription-based offerings that are better suited for operating expenditure (op-ex) models, versus capital expenditure models (standard hardware purchases) that require upfront payment.
- Flexible deployment options can easily scale to provide key management at remote facilities or in cloud infrastructures.
- A newly designed GUI for the k170v model provides a clean, simple, user-friendly experience for commonly used functions like key management, user groups and permissions, and audit log review.

Centralized Key Management:

- 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 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	**k170v** NEW	**k450v**	**k150v**
Max Keys	25,000	1,000,000	25,000
Max concurrent Clients per Cluster	100	1,000	100
FIPS 140-2 Support	L3 with HSM integration	L1 L3 with HSM integration	L1 L3 with HSM integration
HSM Integration *	Yes	Yes	Yes
Supports SafeNet Data Protection Connectors **	SafeNet ProtectApp, SafeNet ProtectV, SafeNet ProtectDB and SafeNet Tokenization	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	Yes
CPU	2 CPU Required	12 CPU (Configurable)	1 CPU Required
RAM	4 GB RAM (Configurable)	8192 MB (Configurable)	1024 MB Ram Required
Network Adapter	1 Allowed/Available	2 (Configurable)	1 Allowed / Available
Interface / Architecture	REST API NAE-XML KMIP	NAE-XML KMIP	NAE-XML KMIP
Supported Cloud Environments	AWS, MS Azure, VMware vSphere, Oracle VM Virtual Box and OpenStack	Can be hosted on a virtual machine running VMware or rented from a service such as AWS Marketplace	Can be hosted on a virtual machine running VMware or rented from a service such as AWS Marketplace
Gemalto Third-party Integration Support	**Content Management:** Open Text (EMC InfoArchive), Stealth Content Store, ServiceNow, VMcrypt **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:** Amazon Web Services S3, DropBox, Google Cloud Storage, Google Drive, IBM ICDES, Panzura Storage Controller **Hyperconvergence:** Nutanix, NetApp Cloud ONTAP, NetApp AltaVault , Cisco UCS, Cisco HyperFlex, vSAN **Cloud Access Security Brokers:** CipherCloud, SkyHigh Networks, Perspecsys (Blue Coat), Hitachi Sepaton VTL, CSC ServiceMesh, Netskope Active Encryption, Vaultive Cloud Data Protection Platform, Elastica (Symantec CASB), Alfresco Open ECM **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, HashiCorp Vault **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, 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 k150v and k450v 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 https://safenet.gemalto.com/contact-us/

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free