

# SafeNet Virtual KeySecure



## Overview

SafeNet Virtual KeySecure™ is a hardened virtual security appliance that provides organizations with a more operation and expense friendly 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

Thales's latest SafeNet Virtual KeySecure models are the k170v and k470v, which are built on prevailing cloud-based technologies and provide a cloud friendly, key management solution for your organization.

With a REST interface and microservices based architecture, new generation models have 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 private and public cloud infrastructures.

## 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 diverse encryption solutions, including the SafeNet Data Protection portfolio, traditional storage and hyperconvergence solutions, Big Data, KMIP compliant solutions, and many others. Thales offers a virtual key management appliance that can also be integrated with a hardware root of trust.

# SafeNet Virtual KeySecure benefits

## Host Anywhere:

- The k150v and k450v models can be rented from a service such as AWS marketplace, or hosted on a virtual machine such as VMware.
- New! The new k170v and k470v models provide additional hosting options, and can run as a native virtual machine on VMware, AWS, Microsoft Azure, Oracle VM Virtual Box, OpenStack, Microsoft Hyper-V and Google with more public/private clouds coming soon.

## Compatibility:

- Compatibility with the OASIS Key Management Interoperability Protocol (KMIP) standard provides support for a large and large and growing partner ecosystem.
- 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 Thales (available for all models).

## Flexibility:

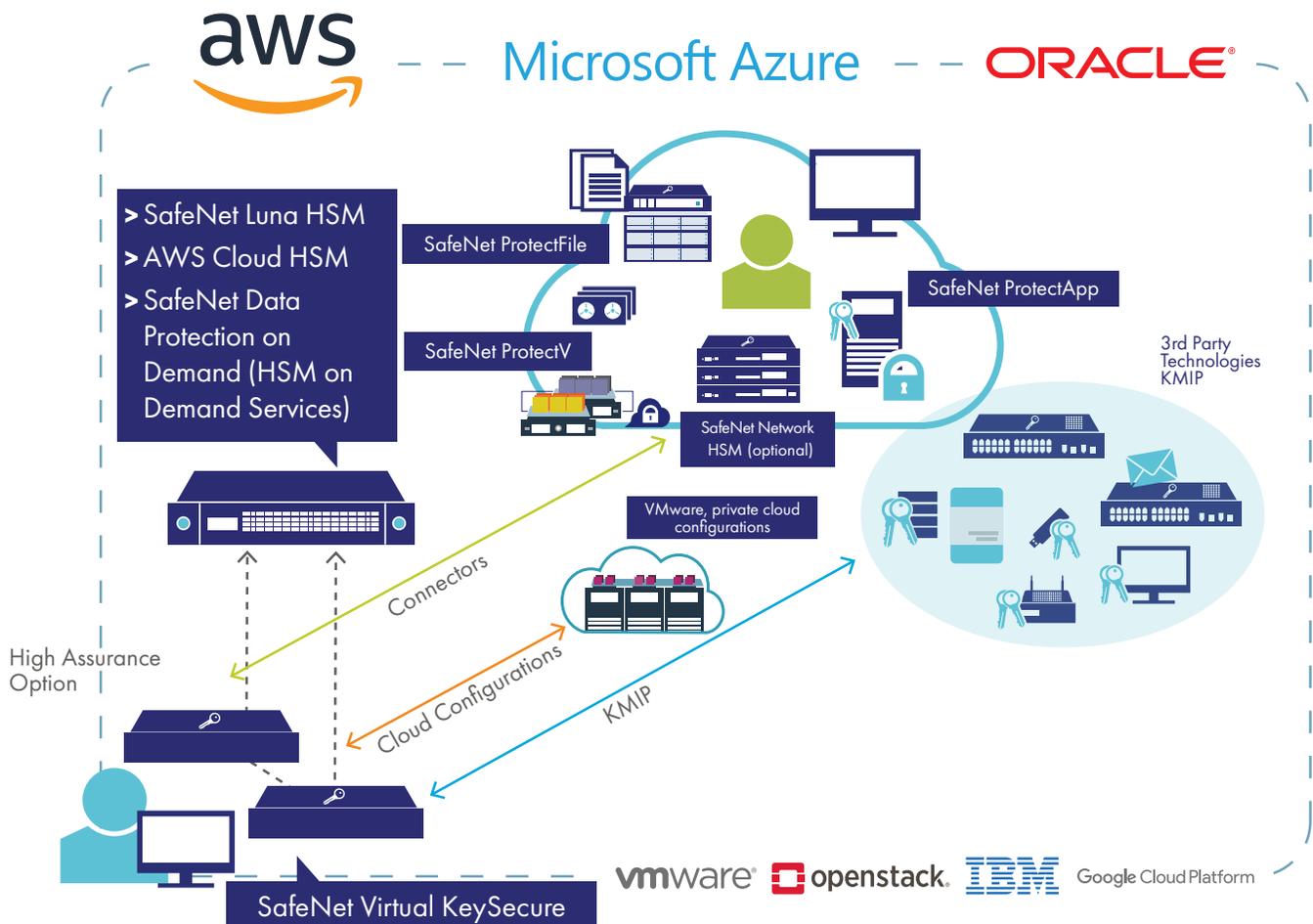
- Subscription-based offerings that are better suited for operating expenditure (op-ex) models, versus capital expenditure models (standard hardware purchases) that require upfront payment.
- Flexible deployment options can easily scale to provide key management at remote facilities or in cloud infrastructures.
- A newly designed GUI for the k170v and k470v models 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 Thales and third-party encryption products across stored and archived data, virtual workloads, and application data protection.



## Virtual KeySecure model comparison

SafeNet Virtual KeySecure				
	NEW k170v	NEW k470v	k450v	k150v
<b>Max concurrent Clients per Cluster</b> ***	100 clients per cluster and 1,000 connections	1000 clients per cluster and 7000 connections	1,000 clients per cluster and 7,000 connections	100 clients per cluster and 1,000 connections
<b>FIPS 140-2 Support</b>	L3 with HSM integration	L3 with HSM integration	L1, L3 with HSM integration	L1, L3 with HSM integration
<b>HSM Integration *</b>	SafeNet Luna HSM 5, 6, 7, AWS Cloud HSM & SafeNet DPoD (HSM On Demand Services)	SafeNet Luna HSM 5, 6, 7, AWS Cloud HSM & SafeNet DPoD (HSM On Demand Services)	SafeNet Luna HSM 5, 6	SafeNet Luna HSM 5, 6
<b>Supports SafeNet Data Protection Portfolio **</b>	SafeNet ProtectApp, SafeNet ProtectV, SafeNet ProtectDB, SafeNet Tokenization, SafeNet ProtectFile, SafeNet High Speed Encryptors, SafeNet Sure Drop, Oracle TDE and SQL Server EKM			
<b>Supports KMIP</b>	Yes	Yes	Yes	Yes
<b>CPU (Minimum Requirements)</b>	2	4	12	1
<b>RAM (Minimum Requirements)</b>	4 GB	8 GB	8192 MB	1024 MB
<b>Network Adapter</b>	1 Allowed / Available	Configurable (2 or More)	2 (Configurable)	1 Allowed / Available
<b>Interface / Architecture</b>	REST API NAE-XML KMIP	REST API NAE-XML KMIP	NAE-XML KMIP	NAE-XML KMIP
<b>Supported Cloud Environments</b>	AWS, MS Azure, VMware vSphere, Oracle VM Virtual Box, OpenStack, Microsoft Hyper-V and Google	AWS, MS Azure, VMware vSphere, Oracle VM Virtual Box, OpenStack, Microsoft Hyper-V and Google	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
<b>Thales Third-party Integration Support</b> <i>(Support for k170v and k470v underway, please contact your Thales account representative for more details.)</i>	<p><b>Content Management:</b> Open Text (EMC InfoArchive), Stealth Content Store, ServiceNow, VMcrypt</p> <p><b>Mainframe Encryption:</b> PKWARE</p> <p><b>Big Data:</b> Dataguise, DataStax, Hadoop, MongoDB, MariaDB, SAP HANA, Cassandra, Couchbase, Hortonworks, Cloudera</p> <p><b>Analytics:</b> IBM QRadar, HPE ArcSight, Splunk, RSA Security Analytics, Above Security</p> <p><b>Application Servers:</b> IBM WebSphere, Oracle Weblogic, Microsoft IIS, Apache Tomcat, Red Hat JBoss</p> <p><b>Backup Solutions:</b> Commvault Simpana, Symantec NetBackup (via NetApp)</p> <p><b>Cloud Storage:</b> Amazon Web Services S3, DropBox, Google Cloud Storage, Google Drive, IBM ICDES, Panzura Storage Controller</p> <p><b>Hyperconvergence:</b> Nutanix, NetApp Cloud ONTAP, NetApp AltaVault, Cisco UCS, Cisco HyperFlex, vSAN</p> <p><b>Cloud Access Security Brokers:</b> CipherCloud, SkyHigh Networks, Perspecsys (Blue Coat), Hitachi Sepaton VTL, CSC ServiceMesh, Netskope Active Encryption, Vaultive Cloud Data Protection Platform, Elastica (Symantec CASB), Allfresco Open ECM</p> <p><b>Databases:</b> MS SQL Server (EKM), Oracle (TDE), IBM DB2, Oracle MySQL, Oracle Database, Teradata</p> <p><b>File and Disk Encryption:</b> PKWARE, IBM, Dell, AWS, Microsoft, LUKS, ViaSat</p> <p><b>Identity Management:</b> Centrify Privilege Service, Lieberman Software</p> <p><b>Key Managers:</b> Hadoop KMS, Cloudera Navigator Key Trustee Server, HashiCorp Vault</p> <p><b>Physical Storage:</b> 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 &amp; i40/80),Viasat, Brocade FS8-18, Huawei Oceanstor, Tintri VMStore, NexentaStor 4.5</p>			

\*Supports master key storage as a root of trust in HSMs: Cloud-based, such as Amazon Web Services CloudHSM, SafeNet Data Protection on Demand (HSM on Demand Services), or SafeNet Luna HSM, a hardware appliance option that is deployed on-premises in a range of models and configurations.

\*\*SafeNet Virtual KeySecure k150v and k450v appliances using SafeNet ProtectApp, SafeNet ProtectDB, and SafeNet Tokenization, require the purchase of SafeNet Crypto Pack. SafeNet ProtectV and SafeNet ProtectFile do not require SafeNet Crypto Pack feature activation. The k170v and k470v using any of the SafeNet Data Protection portfolio do not require the purchase of SafeNet Crypto Pack.

\*\*\*Based on physical/virtual default system environments. Based on an average client test, performance will vary depending on use case and configuration.

## 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.

## About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

### 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](#).