PRODUCT BRIEF

Gemalto 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 does not fit some budgets.

SafeNet Virtual KeySecure™ is a hardened virtual security appliance that provides a more operation- and expense-friendly alternative. 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. SafeNet Virtual KeySecure allows customers to manage keys, unify encryption, and enforce access control across these virtualized and 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, remote data management a challenge. With regulations such as PCI DSS, HIPAA/HITECH, 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. Like its hardware counterpart, SafeNet Virtual KeySecure is capable of managing up to 25,000 keys and 100 maximum concurrent clients per cluster. SafeNet is the only solutions provider that offers a virtual key management appliance integrated with hardware root of trust (using SafeNet Luna Hardware Security Modules 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.
> Bring Your Own License (BYOL) for AWS Marketplace enables purchase of Connector licenses directly from SafeNet.
> Hourly or annual 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 Features and Benefits

SafeNet Virtual KeySecure is a subscription-based, virtual solution that provides flexible, secure key management and also helps meet the most stringent security and compliance requirements. SafeNet Virtual KeySecure ensures that organizations maintain ownership of their encryption keys at all times by hardening the appliance OS and encrypting the entire virtual appliance.

SafeNet Virtual KeySecure Features and Benefits

Features	Benefits
Hardened Virtual Appliance	> Centralized key management for virtual appliance > 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 Cloud HSM Service > Accelerated deployments
Field Proven Key Management	> Enterprise key management leader > High availability to support cloud scale deployments > Proven performance profile > Heterogeneous key management including self-encrypting drives, tape archives, storage area networks, virtual workloads, and more, including support for the OASIS Key > Management Interoperability Protocol (KMIP) standard > Centrally manages multiple key types: symmetric, asymmetric, secret data, and X.509 certificates
Cost Efficient	> Subscription-based model fits many budgets; eliminates need for additional rack space > Support for OASIS KMIP standard enables increased centralization of encryption key management over time > Available through pay-as-you-go subscription model
Compatibility	> **Gemalto SafeNet Crypto Pack:** Encrypts structured or unstructured sensitive data residing in virtual data centers. > **HSMs:** For maximum security, supports key storage in hardware security modules (HSMs) such as Amazon Web Services CloudHSM in a subscription-based AWS environment, and SafeNet Luna SA HSM, a hardware appliance option that is deployed on-premises in a range of models and configurations > **VMware:** private cloud configurations > **Storage Devices:** Supports many popular NAS, tape, and backup storage devices from NetApp, IBM, Hitachi Data Systems, Dell, Brocade, Quantum, and more > **KMIP:** Supports the Key Management Interoperability Protocol, allowing customers to consolidate key security policies across disparate encryption systems, including storage devices, cloud encryption gateways, and more contents of your virtual machine and leverage the benefits of virtual storage while retaining access control and ensuring privacy of your data.

SafeNet Virtual KeySecure Use Cases

SafeNet Virtual KeySecure provides application data protection and centralized key management for SafeNet and third-party encryption products across stored and archived data, virtual workloads, and application data protection.
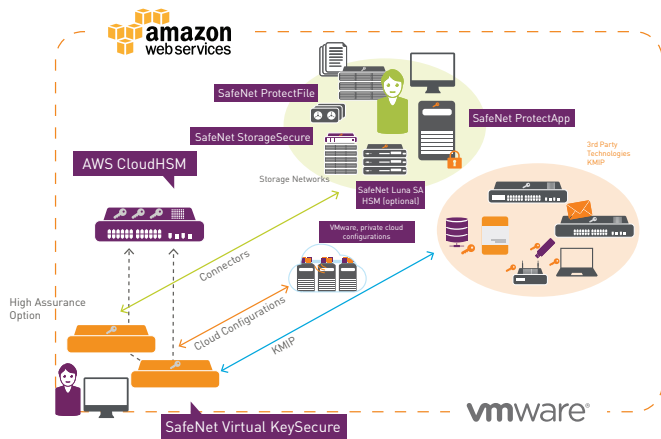
About Gemalto's SafeNet Identity and Data Protection Solutions

Gemalto's portfolio of SafeNet Identity and Data Protection solutions enables enterprises, financial institutions and governments to protect data, digital identities, payments and transactions–from the edge to the core. Our solutions take a data-centric approach to security with innovative encryption methods, best-in-class crypto management, and strong authentication and identity management to help customers protect what matters, where it matters.

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.

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 www.safenet-inc.com
Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free