SafeNet | THE DATA PROTECTION COMPANY

Crypto Operations Upgrade Pack

PRODUCT BRIEF

SafeNet KeySecure with Crypto Pack Benefits

Operational Efficiency
- Lower the operational impact of encryption by offloading processor intensive symmetric encryption tasks to a dedicated appliance

Lower Administration Costs
- Lowers the costs of encryption and key management with centralized administration and automated operations

Simplified Compliance
- Centralized, efficient auditing of encryption and key management practices saves staff time and decreases the time spent on compliance mandates

Lower Total Cost
- Low TCO is ensured with layered encryption options from SafeNet and key management

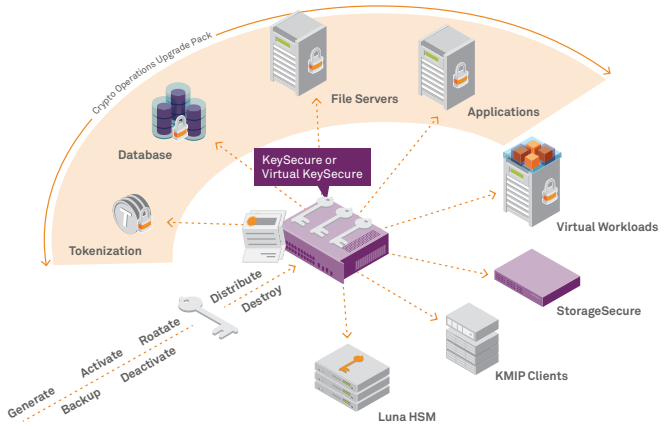
Security and Compliance for Virtualized Environments
- Take advantage of the lower costs of virtualized and cloud environments with flexible deployment options and appliance models covering physical and virtualized (VMware) environments

Risk Mitigation with Maximum Key Security
- Tamper-proof hardware options and hardened virtual appliance for securing encryption solution

TurnKey Encryption

In conjunction with SafeNet KeySecure for security policy and key management, SafeNet's Crypto Operations Upgrade Pack (Crypto Pack) enables KeySecure to be used for encryption of structured or unstructured sensitive enterprise data residing in a server in the data center (physical, virtual, or cloud-based) or in the distributed enterprise. Data can be encrypted at the application, database column, file-system, virtual machine, or storage levels.

Crypto Operations Upgrade Pack Solutions



Crypto Pack Solutions Include:

Application Level Encryption

SafeNet ProtectApp provides encryption of sensitive data in applications and keeps it secure across its entire lifecycle – no matter where it is transferred, backed up, or copied. Using ProtectApp APIs, applications have the ability to protect both structured and unstructured data in a multi-vendor application server infrastructure in a data center and the cloud. Encrypted data can only be decrypted by authorized users within an application.

Through its integration with KeySecure, ProtectApp offers centralized administration of application encryption policy and keys. Encryption processes can also be offloaded to KeySecure for improved security.

- Web application servers supported: Apache Tomcat, IBM WebSphere, JBoss, Microsoft IIS, Oracle WebLogic, SAP, NetWeaver, Sun ONE, and more
- APIs supported: KMIP, ICAPI, JCE, MS-CAPI, .NET, PKCS #11

Database Column Level Encryption & Tokenization

SafeNet ProtectDB provides transparent, column-level encryption of sensitive data in multi-vendor database management systems. Only authorized users or applications can successfully access sensitive data in encrypted columns within the database.

Supported Technologies

Cryptographic Algorithms
- 3DES, AES, DES, RSA (signature and encryption), RC4, SHA-1, HMAC

Asymmetric Key Sizes
- 512, 1024, 2048, 3072, 4096

Symmetric Key Sizes
- 40, 56, 112, 128, 168, 192, 256, 384

Databases
- IBM DB2, Microsoft SQL Server and Oracle

Applications and Web Servers
- BEA, IBM, IIS, Oracle, Apache, JBoss, SAP and PeopleSoft

API Support
- KMIP, ICAPI, JCE, MS-CAPI, .NET, PKCS #11

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

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

Authentication
- LDAP and Active Directory

Through its integration with KeySecure, ProtectDB offers centralized key and policy management and policy control of data access with granular restriction options and regular key rotation. In addition, the solution enables segregation of data within a database, strong separation of duties, and the ability to meet compliance mandates.

- Databases supported: Oracle, Microsoft SQL Server, IBM DB2

SafeNet Tokenization Manager protects sensitive information in databases by replacing it with a surrogate value that preserves the length and format of the data. Highly scalable and cost-effective solution to implement.

Through its integration with KeySecure, Tokenization Manager provides a single, centralized interface for logging, auditing, and reporting access to protected data, keys, and tokens.

- Supported token vault databases: Microsoft SQL Server, Oracle
- Supported APIs: Java, Web Service

Note: all tokenization forms are supported on all databases as long as the vault itself is on Microsoft SQL Server or Oracle.

File-system Level Encryption

SafeNet ProtectFile provides transparent and automated file-system level encryption of server data-at-rest in the distributed enterprise, without disruption to business operations, application performance, or end-user experience.

Through its integration with KeySecure, ProtectFile offers centralized key and policy management, segregation of data on shared servers, strong separation of duties, and the ability to meet compliance mandates.

- Platforms supported: Linux (Red Hat Enterprise, Suse, Oracle Unbreakable Enterprise Kernel), Microsoft Windows, Apache Hadoop

Additional Encryption Options

SafeNet KeySecure also supports additional solutions for the encryption of unstructured data at the virtual machine and storage level, including:

Virtual Machine Level Encryption

SafeNet ProtectV delivers full disk encryption of virtual instances and attached storage volumes to enable the secure migration of sensitive and highly regulated data to the cloud or a virtual data center.

Through its integration with Virtual KeySecure, ProtectV provides the ability to separate security administration duties, enforce granular controls, and establish clear accountability with audit trails and detailed compliance reporting.

- Cloud platforms supported: AWS EC2, Amazon VPC, VMware vSphere

Storage Level Encryption

SafeNet StorageSecure encrypts information based on defined business policies in an all inclusive, secure hardware storage encryption device, and protects shares, folders and files on any Network Attached Storage (NAS) filers.

Through its integration with KeySecure, StorageSecure offers secure, geographically distributed management of keys, and provides centralized key management.

- Directory services supported: Microsoft Active Directory, LDAP, NIS, Radius

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/news-media