

# SafeNet DataSecure

## PRODUCT BRIEF

### SafeNet DataSecure 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 key management practices saves staff time and decreases the time spent on compliance mandates
- **Lower Total Cost of Ownership.** Low TCO is ensured with layered encryption options from SafeNet and key management supporting a growing list of encryption products using the OASIS KIMP standard so that current and future needs are addressed
- **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

### Overview

SafeNet DataSecure centralizes cryptographic processing, security policy and key management with a range of hardware and hardened virtual appliances. Only SafeNet delivers tokenization and encryption at the application, database, file and virtual workload level in a high-availability solution that easily deploys in traditional and virtualized data centers or service provider environments.

### Highlighted Capabilities

- **High Performance Encryption.** DataSecure's proven cryptographic performance means critical encryption tasks can be offloaded to a dedicated appliance that ensures data protection efforts do not impede critical IT operations.
- **Heterogeneous Key Management.** Manages keys for a variety of encryption products including self-encrypting drives, tape archives, Storage Area Networks, virtual workloads, applications and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.
- **Multiple Key Types.** Centrally manages symmetric, asymmetric, secret data, and X.509 certificates along with their associated policies.
- **Full Lifecycle Key Support and Automated Operations.** Simplifies the management of encryption keys across the entire lifecycle including secure key generation, storage and backup, key distribution and key deactivation and deletion. DataSecure 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 administrators are restricted roles defined for their scope of responsibilities.
- **High-Availability and Intelligent Key Sharing.** Deploys in flexible high-availability configurations within an operations center and across geographically dispersed centers or service provider environments using an active-active mode of clustering.
- **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.

### SafeNet DataSecure i460, i450 and i150

SafeNet DataSecure i460, i450 and i150 provide high performance symmetric encryption and centralized key management in a range of FIPS 140-2 level 3 (using an embedded Luna HSM) and level 2 validated appliances.

## Supported Technologies (All Models):

### Cryptographic Algorithms

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

### Asymmetric Key Sizes

- 512, 1024, 2048, 3072, 4096

### Symmetric Key Sizes

- 40, 56, 128, 168, 192, 256

### Databases

- IBM DB2, Microsoft SQL Server and Oracle

### Applications and Web Servers

- BEA, IBM, IIS, Oracle, Apache, JBoss, SAP and PeopleSoft

### API Support

- KMIP 1.1, PKCS #11, JCE, MS-CAPI, and .NET

### 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

### Hardware Specifications:

#### DataSecure i460

- Two (2) 10/100/1000 Mbps Network Interfaces
- Eight cooling fans
- Two 502W Energy Smart power supplies
- 1U, rack mountable (H: 1.7"; W: 19"; D: 30")

#### DataSecure i450

- Two (2) 10/100/1000 Mbps Network Interfaces
- Five cooling fans
- Two 502W Energy Smart power supplies
- 1U, rack mountable (H: 1.7"; W: 19"; D: 30")

#### DataSecure i150

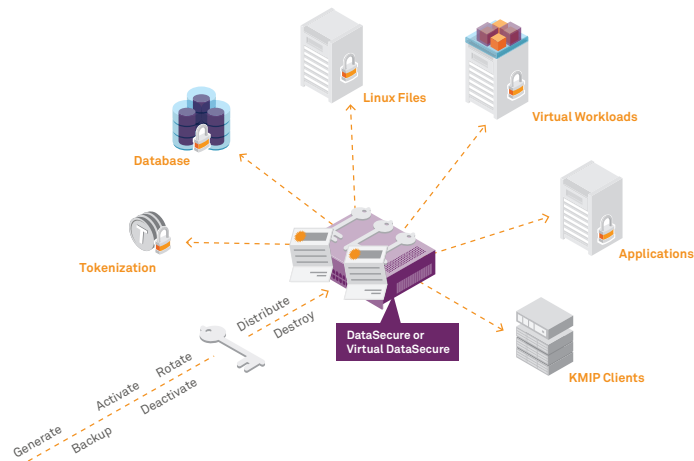
- One (1) 10/100/1000 Mbps Network Interface
- One cooling fans
- 250W, 100 - 240 VAC, auto-ranging, 50-60 Hz, 5 - 3A power supply
- 1U, rack mountable (H: 1.7"; W: 19"; D: 13")

## Virtual DataSecure i150v

SafeNet Virtual DataSecure, a hardened virtual security appliance, provides security and centralized management of encryption keys used for the protection of sensitive data in virtualized and cloud environments. Virtual DataSecure is quickly deployed for high-availability in virtualized infrastructures. With Virtual DataSecure organizations get:

- Dedicated cryptographic processing and key management in virtual security appliance for VMware (ESXi 4 and 5)
- Hardened OS and complete virtual appliance encryption for enhanced key security
- Accelerated deployments - simply power on the virtual appliance

## DataSecure Use Cases



SafeNet DataSecure use cases cover SafeNet tokenization and layered encryption products across application, file, database and virtual workload data protection. In addition, DataSecure supports key management for a broad eco-system of third party products using the KMIP standard.

## SafeNet DataSecure Model Comparison

Feature	DataSecure i460	DataSecure i450	DataSecure i150	DataSecure i150v
Performance	100,000 encryptions per second		8,000 encryptions per second	
Capacity	Up to 1,000,000 keys and cryptographic objects per cluster		Up to 25,000 keys and cryptographic objects per cluster	
Max concurrent clients	1,000 per cluster		100 per cluster	
FIPS 140-2 Level 3	Yes (Embedded Luna HSM)	No	No	N/A
FIPS 140-2 Level 2	Yes	Yes	Yes	N/A
Supported SafeNet Connectors:	ProtectApp, KMIP, ProtectDB, ProtectV, ProtectFile for Linux and Tokenization Manager supported on all			
SafeNet Third-party Integration Support	HP ESL G3, Quantum Scalar Series(i6000, i500 & i40/80), NetApp NSE, Hitachi VSP, Amazon Web Services S3, DropBox, Google Cloud Storage, Google Drive			
Partner Integration Support (requires ProtectApp)	CipherCloud, Perscesys, PKZip, Sepaton VTL, ServiceMesh, Viasat			

**Contact Us:** For all office locations and contact information, please visit [www.safenet-inc.com](http://www.safenet-inc.com)

**Follow Us:** [www.safenet-inc.com/connected](http://www.safenet-inc.com/connected)

©2013 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. PB (EN)-10.15.13