Gemalto's SafeNet Key Secure Solutions for Dell Storage SC Series – *Working Together to Secure Data-at-Rest.*

Data-at-rest security solutions need to ensure that data is secured from unauthorized users and that it remains under full customer control at all times. Dell Storage SC Series self-encrypting drives (SED) secure data so only holders of the appropriate authorization key can access it. Gemalto's SafeNet KeySecure provides customers with complete control by securing the keys needed to access the SEDs. Together, Dell and Gemalto offer a secure, and efficient means of securing data at rest with encryption.

Centralized Management of Access Keys

- Centralize and simplify key management (e.g., escrow, recovery) for all SC Series self-encrypting drives and KMIP-compatible encryption solutions, while improving compliance and auditability.

High-Availability Configurations

- Cluster multiple KeySecure appliances to maintain encrypted data availability, even in geographically dispersed data centers.

Separation of Duties

- KeySecure supports segmented key ownership and management

Encryption is fundamental to any defense-in-depth strategy whether the goal is compliance or securing sensitive data. Self-encrypting drives are an effective way to deploy encryption in large-scale storage environments. However, as the number of drives increases, so does the number of encryption keys, key stores, and access policies needing management. The administrative effort involved in managing these deployments and the associated key lifecycle is significant, and can become unwieldy as encryption use increases. To cost-effectively support such an environment and bring it into regulatory compliance, enterprise key management must be part of the solution.

Solution

Centralizing the storage of access keys to the self-encrypting drives (SEDs) not only simplifies key management, but also ensures that encrypted data is protected from unauthorized access—even as the size of the encryption deployment grows. Dell Storage self-encrypting drives ensure that data stored on those drives are secure. Gemalto's SafeNet KeySecure™ integrates with Dell Storage SC Series Secure Data solutions to provide robust, enterprise-scale key management, ensuring that access keys are managed throughout their lifecycle and properly secured with FIPS 140-2 certified hardware.

Dell Storage

Dell Storage SC Series arrays (including Dell Compellent solutions) optimizes data throughout its lifecycle via built-in intelligence that automatically places data on drives according to its level of use. The SC Series is a high-performance, efficient, and scalable platform based on a modular architecture that unifies block and file to help lower total cost of ownership. Real-time system information about each data block allows SC Series arrays to optimize placement, management, and protection throughout the lifecycle. In addition, SC Series secures data from unauthorized access through the use of FIPS 140-2 Level 2-compliant self-encrypting drives using the Advanced Encryption Standard (AES-256) algorithm.

Gemalto SafeNet KeySecure

Gemalto SafeNet KeySecure is a key management appliance that integrates with Dell Storage via the Key Management Interoperability Protocol (KMIP) to store and centralize the management of the Authority Credentials (sometimes referred to as the locking, authentication or access keys) for

Gemalto SafeNet KeySecure Appliances:

k460:

Gemalto's SafeNet KeySecure k460 is the highest-capacity, highest-performing key manager in the KeySecure portfolio. The k460 is ideal for organizations requiring high levels of both scalability and security. Compellent SEDs using KeySecure mitigate the threat of unauthorized access to encrypted data at rest on powered-off disk drives. The k460 offers:

- A resilient appliance with redundant hot-swap hard drives and power supplies
- FIPS 140-2 Level 3-certified security
- Key management for large environments with a significant number of SEDs, or other devices requiring key storage

k250:

Gemalto's SafeNet KeySecure k250 physical appliance is designed for small to medium size businesses requiring strong key management security without the scale and performance capacity offered by the k460. Since these appliances are FIPS 140-2 Level 1-certified, this option is suitable for organizations subject to fewer regulations concerning their data security. The k250 offers:

- FIPS 140-2 Level 1 security
- Cost-effective key management

k150v:

Gemalto's SafeNet k150v, or Virtual KeySecure, is a software-based virtual key manager that is ideal for smaller Compellent SED deployments, remote sites or virtualized environments. The k150v provides strong key security, ensuring that customers maintain control of their acess keys even as they migrate to the cloud. Virtual KeySecure offers the same key storage capacity as the k250 to allow the same level of scalability in virtual environments as a customer would have when deploying an entry on-premise key management option. The k150v offers:

- A solution tailored to the needs of virtualized data centers and public cloud environments
- Cost-effective key management

Installation and Support

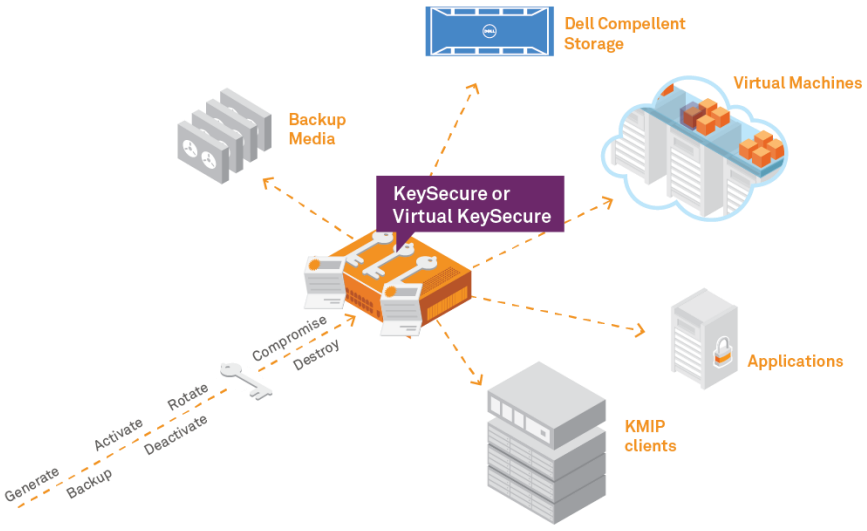
To ensure successful deployment, Gemalto's Professional Services team schedules on-site visits to install KeySecure and get the customer up and running. In addition, Gemalto offers comprehensive on-going support packages in 1 and 3 year terms that cover mission critical business and operational issues. Throughout KeySecure's lifecycle, Gemalto support is committed to ensuring customer satisfaction.

Conclusion:

Encrypting data in the storage environment is critical to ensuring that data is safe in the event of a security breach. Dell and Gemalto combine to offer organizations the ability to secure data through encryption without making the management of the necessary encryption keys and policies unwieldy or difficult.

For more, visit: http://www.safenet-inc.com/partners/dell.

KeySecure in Dell Compellent Deployments



SafeNet KeySecure Model Comparison

	KeySecure		
Feature	**k460**	**k250**	**k150v**
Max keys	1,000,000	25,000	25,000
Max concurrent clients per cluster	1,000	100	100
Redundant hot-swap HDs & Power	Yes	No	N/A
FIPS 140-2 Support	Level 3	Level 1	Level 1
HSM Integration*	Yes	Yes	Yes
SafeNet Crypto Pack**	Optional	Optional	Optional
SafeNet StorageSecure	Yes	No	No
SafeNet Third-party Integration Support	Application Servers: Apache Tomcat, IBM WebSphere, JBoss, Microsoft IIS, Oracle WebLogic, and more Archive & Tape Libraries: Quantum Scalar (i6000, i500, i40/80), HP ESL G3, HP MSL TL, Sepaton VTL Cloud Encryption Gateways: Perspecsys , CipherCloud, Skyhigh Secure, ServiceMesh Cloud Storage: AWS S3, AWS EC2/VPC, Google Cloud Storage, Google Drive, Dropbox, Hitachi VSP G1000, Nutanix File and Disk Encryption: PKWare PKZip Physical Storage: NetApp NSE, Dell Compellent, IBM XIV, Brocade BES & FS8-18 Blade Server, Hitachi RAID700, Hitachi HUS-VM, Hitachi HUS 100, HP XP7 9000, HP 3PAR		

* KeySecure will integrate with both Luna SA and Amazon CloudHSM