Feature Brief

Dell Storage SC Series Secure Data Solutions

Intelligent choice for data-at-rest encryption and compliance

Who needs data-at-rest security?

- Healthcare
- Finance/Banking
- Government/Education
- Any business with significant intellectual property

Why SEDs?

- Government-certified solution
- Encrypts everything on drive
- Auto-locks on power-down or removal
- SecureErase eliminates risk when drives are repurposed
- Transparent to users and applications
- No performance penalty

Why Dell Storage SC Series?

- Intelligent tiering and optimization in an encrypted environment
- No new array hardware required
- Incremental roll-out with SEDs and standard drives in same array
- Industry-standard Key Management service support

As security breaches in both government and private sector environments continue to make headlines, organizations of all kinds are focusing on data protection. IT managers and CEOs alike know just how quickly valuable customer relationships and overall business goals can be jeopardized by information theft, loss or unauthorized access — not to mention the hefty fines resulting from regulatory non-compliance.

Although major investments have been made to safeguard data at the network and host level, security analysts increasingly warn of “data at rest” vulnerabilities in the storage media itself — which is where information spends most of its lifecycle. Fortunately, to address these concerns, trusted, widely-implemented solutions now exist that leverage full-disk encryption (FDE) technology and the next generation of self-encrypting drives (SEDs) to provide failsafe security options directly within the storage array.

Physical protection, zero performance penalty

SEDs use advanced cryptography to eliminate the risk associated with physically stolen or inappropriately retired drives. SEDs removed from the system are automatically locked, and without their individual encryption keys, remain 100 percent unreadable — even if disassembled and placed on a “spin stand.” When redeployed in another array, SEDs are cryptographically erased, a much quicker and more thorough method than simply degaussing or overwriting the drives.

Unlike software-based encryption, SED security is built into each drive and cannot be turned off. No external mechanisms are required to encrypt and decrypt the data, which means the solution remains completely transparent to users and applications. In addition, Dell’s SEDs have no impact on system, network or workload performance — you simply install and use them like any other storage media.

Meets stringent regulatory requirements

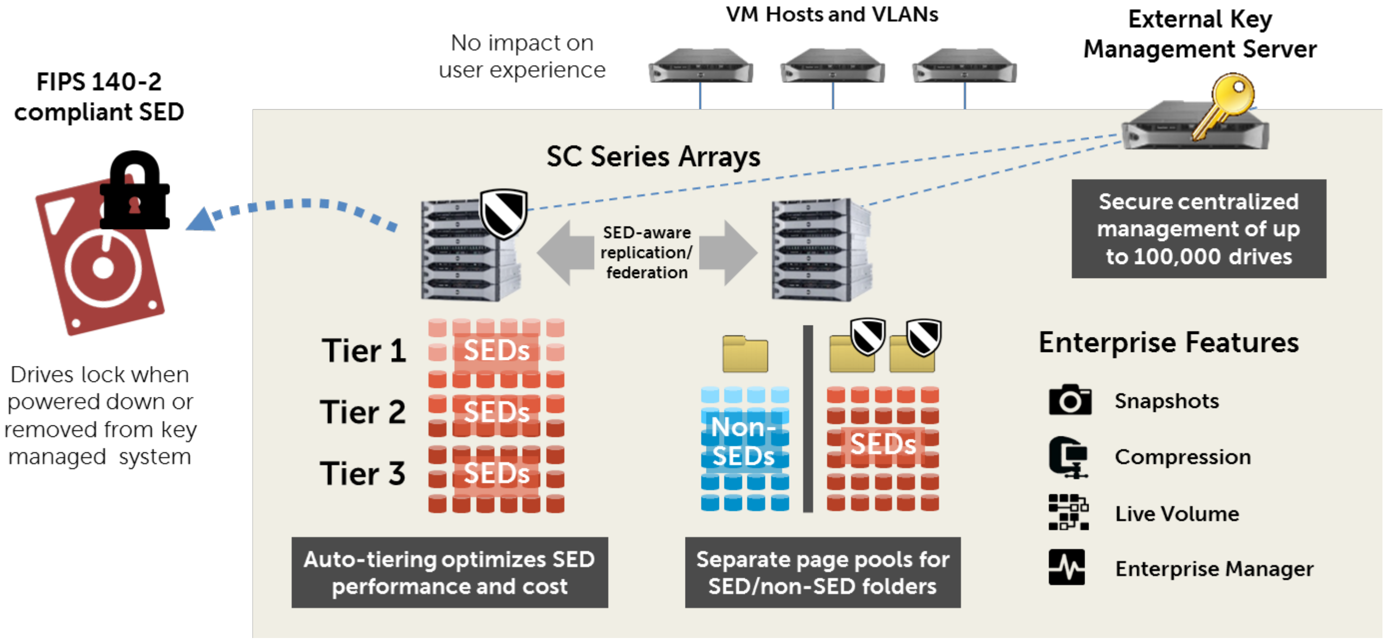
Government agencies recognize the power of data-at-rest security solutions, and have established FDE standards to encourage or mandate their use. Dell SC Series arrays support the most important certifications, including the critical FIPS 140-2 levels required for sales into secure government data centers.

Cost-effective, easy to implement

Dell makes this leading technology practical and affordable with flexible solutions that let you control the timeline and scope of your SED deployment. While other solutions require all media be either secure or non-secure, SC Series’ ability to support SED and standard drives in the same array enables a “pay as you go” approach to encryption. You can apply SEDs incrementally to specific volumes only, with discrete page pools providing full separation for locked versus unlocked LUNs. No need to overcommit now — with the SC Series, you can start with an SED proof-of-concept, or add end-to-end protection to an entire array at any time.

Security plus storage optimization

Best of all, with Dell's solution, you don't have to give up or degrade the world-class enterprise features that made you choose SC Series in the first place. All the intelligent and popular Storage Center advantages, including Data Progression, Data Instant Replays, and Live Volume, remain fully available when you add SEDs. Encryption has no negative impact on these capabilities, although it is fully-integrated with the SC Series management toolset. The Enterprise Manager administrative console, for example, provides "SED aware" guidance to ensure your secure data *remains* on secure drives, even following replication, migration or federation.


FIPS 140-2 compliant SED
Drives lock when powered down or removed from key managed system
No impact on user experience
VM Hosts and VLANs
External Key Management Server
SC Series Arrays
SED-aware replication/ federation
Secure centralized management of up to 100,000 drives
Tier 1
SEDs
Tier 2
SEDs
Tier 3
SEDs
Non-SEDs
SEDs
Auto-tiering optimizes SED performance and cost
Separate page pools for SED/non-SED folders
Enterprise Features
Snapshots
Compression
Live Volume
Enterprise Manager

What do I need to get started with a SC Series Secure Data Solution?

1. **Secure Data array license** — Simply apply the cost-effective Secure Data license to your current or previous-generation SC Series array.[1] No forklift upgrade or I/O card installation is required, unlike other solutions which can require an entirely new array. The one-time license covers any number of drives, no matter how large your system grows, and as with other SC Series software, may be transferred to different arrays as you evolve your environment. Secure Data licensing automatically enables the array for Key Management Interoperability Protocol (KMIP) standardized communication with supported Key Management Server solutions.

2. **Self-encrypting drives (SEDs)** — Dell offers a variety of SED speeds and capacities, available individually or in convenient, value-priced bundles. Each drive includes its own onboard encryption engine to seamlessly encrypt data as it is written and de-encrypt it as it is read. Standard-sized, tamper-proof formats work with current drive carriers, and are fully compliant with FIPS 140-2 Level 2, using the Advanced Encryption Standard (AES-256) algorithm.

3. **Remote Key Management Server (KMS)** — Dell supports a choice of industry-standard KMS solutions for convenient, automated management of up to 100,000 secure drives, keys, key stores and access policies. From all-inclusive standalone appliances to server-installable software, these options make key generation, surveillance, rotation and deletion simple — and also help generate reports for regulatory compliance. All supported KMS solutions are also FIPS 140-2 certified, with available options for Level 1-, 2- or 3-compliant services. Leading platform support will allow many enterprise customers to simply leverage their existing KMS previously purchased to manage keys for secure servers, workstations, tape libraries or other devices.

Technical specifications	
Standards	FDE based on AES-256 Drives: FIPS 140-2 Level 2 (KMS options available for FIPS 140-2 Level 1, 2 and 3)
Supported Key Management Systems	Gemalto's SafeNet KeySecure k460, k250, k150v Thales EMS 200

[1] Includes SC8000 and legacy Compellent S40 arrays. Note firmware upgrade to version 6.5 is required for older SC products. SC4000 Series support will be available in a future firmware release.

Learn More at Dell.com.