

# SCI StorInt™ Dispatch – Brocade080922

## Announcing Brocade new fabric level encryption

This Silverton Consulting (SCI) Storage Intelligence (StorInt™) Dispatch provides a summary of Brocade's recent introduction of their fabric level encryption (FS8-18) blade and 2U standalone switch encryption system.

### Fabric level encryption

Brocade is the first to introduce a fabric encryption blade and switch made especially for securing disk “data-at-rest”. Both the new blade and switch support from 48Gb/s to 96Gb/s of encryption throughput. The FS8-18 blade supports 16-8GFC ports and up to four blades can be supported in one DCX backbone. The switch supports 32-8GFC ports. Both devices have a smart card reader for key initialization and two gigE ports for key synchronization and management.

Historically, key management was a crucial missing link to the use of encryption but nowadays key management systems are available from many IT vendors. Consequently, Brocade's new encryption offerings utilize standard key management systems supplied by other vendors and currently support NetApp's Lifetime Key Manager (LKM) and EMC's RSA key manager (RKM) with HP's Secure Key Manager (SKM) to follow in a subsequent release.

Data-at-rest encryption protects data as it is stored. Currently, Brocade's fabric encryption only supports disk data-at-rest but a follow-on release will support tape data as well. This is in contrast to Cisco's SME which only supports tape media or virtual tape device encryption. Later this year Brocade will support five backup products for tape and VTL operations – IBM TSM 5.4, HP Data Protector, EMC NetWorker 7.3, Symantec NetBackup 6.5, and CommVault Galaxy 7.0.

Other encryption solutions to the disk data-at-rest are already available from such vendors as Seagate for disk drives, EMC for storage subsystems and NetApp/Decru for network appliances. Predating all this was tape encryption from most major tape vendors.

Disk data-at-rest encryption provides a significant addition to tape encryption. Although tape encryption protects media that is often taken offsite and out of data center control, less well understood is that service people can easily walk away with a good working disk and that disk data is not protected unless encrypted. Also, once data is encrypted, anyone listening to the fabric past the encryption will be unable to read the data.

### How it works

Specific LUNs are configured to be encrypted and once configured a fabric encryptor starts a background task, which reads each LUN block, encrypts the data, and writes it back. This background activity uses block maps to indicate whether a LUN block is encrypted or not. When a write happens during this process, the data is automatically

encrypted and the block flagged as encrypted in the block map. Also, each LUN has a unique key.

### **Fabric level encryption concerns**

Deduplication and data compression appliances will necessarily reduce data redundancy. Encrypting data prior to these devices will negate their effectiveness. Always place any encryption behind the deduplication or data compression appliance in the data path

Disk mirroring is another problem area. Fabric level encryption will encrypt data at the primary site, a subsystem will then mirror this data to a secondary site. To use such data effectively will require another encryptor at the secondary site with access to a duplicate or original set of keys used at the primary site for encrypting the LUN.

Also, thin provisioned storage subsystems depend on initialized blocks to never be written until needed. If fabric level encryption is required to rewrite pre-existing blocks into ciphertext, all blocks in a thinly provisioned volume would immediately be written and thereby use up storage space.

Finally, while it is good to have data flowing around your SAN in encrypted form, protection only exists once the data is past the encryptor. Data from the HBA to the SAN and from the SAN entry point to the encryptor blade/switch is still in plaintext and thus vulnerable. As such, follow-on products are needed to support HBA encryption, an area that Brocade intends to address in the future.

### **Announcement significance**

Many security risks exist inside a data center. Tape encryption eliminated one risk to media outside the data center. Disk data-at-rest deals with the other remaining hole for data outside the data center but also starts to address securing the data within the data center as well. There are some issues with using this new fabric encryption but for many it's a significant step in the right direction.

---

---

*Silverton Consulting, Inc. is a Storage, Strategy & Systems consulting services company, based in the USA offering products and services to the data storage community.*