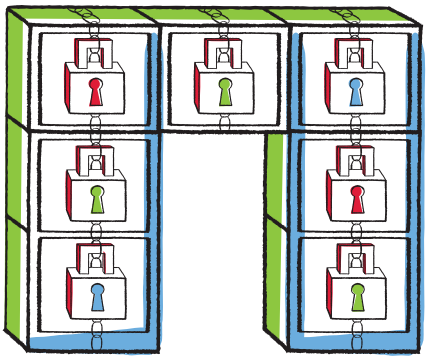

Datasheet

NetApp Storage Encryption (NSE)

Full disk encryption that protects data at rest with no operational impact

KEY FEATURES

Full Disk Encryption
- Self-encrypting drives (SED) prevent data access until the drive's encryption key is unlocked by an authorized administrator

Complete Transparency
- Supports storage efficiency: FAS deduplication and storage compression
- Supports integrated data protection: backup/recovery, SnapMirror®, SnapProtect™, and SnapVault®

Mandatory Data Encryption
- File system and network independent: No action is required by the operator when aggregates, volumes, shares, or LUNs are created or deleted, and your data is always protected

The Challenge

Encrypt your data without getting in the way

You work for a government, financial, or healthcare entity and are subject to regulations surrounding data protection. The requirement to keep all of the personally identifiable information, personal healthcare information, and customer information protected within your storage infrastructure becomes a challenge when repurposing drives, returning defective drives, or upgrading to larger drives by selling them or trading them in. Wouldn't it be nice if there were a way for all of your data to be encrypted all of the time without affecting everyday operations?

The Solution

NetApp Storage Encryption (NSE)

NSE is configured to use self-encrypting drives to facilitate compliance and spares return by enabling the protection of data at rest, through transparent disk encryption. The drives perform all of the data encryption operations internally, including encryption key generation. To prevent unauthorized access to the data, the storage system must authenticate itself with the drive using an authentication key that is established the first time the drive is used. The authentication key is backed up to an external key manager using the industry-standard OASIS Key Management Interoperability Protocol (KMIP). Only the storage system, drive, and key manager have access to the key, and the drive cannot be unlocked if it is moved outside of the security domain, thus preventing data leakage.

Completely Transparent

NetApp fundamentals supported

While higher level SAN and NAS fabric encryption solutions provide more flexibility, they can also present a challenge to everyday operations. Data encrypted before it is sent to the storage module cannot be compressed, deduplicated, or scanned for viruses, and it might need to be decrypted before it can be replicated to a backup site or archived to tape.

Contrast this with NSE, which transparently supports these NetApp® storage efficiency features. NSE can help you lower your overall storage costs, while preventing old data from being accessed if a drive is repurposed.

Set and forget

When new volumes, shares, or LUNs are created in storage using network or fabric encryption, the storage administrator needs to determine that encryption is enabled. Not so with NSE. Data encryption is always on and is completely transparent to any data operations above the physical disk. Once NSE is enabled, it does not matter how

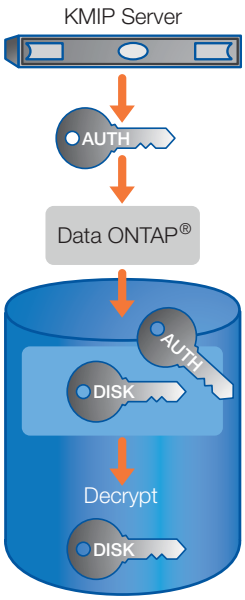

Figure 1) Schematic diagram of NSE key wrapping.

NETAPP STORAGE ENCRYPTION

Encrypts data at rest	●
Supports NetApp storage efficiency	●
Works with NAS encryption	●
Works with SAN encryption	●
Spares return, repurpose drives without data disclosure	●

Table 1) NSE protects disk-based data at rest whether on SAN or NAS, all at wire speed.

your storage is provisioned. Even if you move the drive from one shelf to another or from primary to secondary storage, the data you've placed on it is protected from disclosure.

Industry standard means no disk left behind

Because NSE uses the new cross-platform industry-standard Key Management Interoperability Protocol, you can use our solution with any compatible key manager now and in the future.

Do I Need More than NSE?

Some questions to ask yourself

- Do you need to encrypt data on tape?
- Does data need to be encrypted on the SAN or NAS network?
- Do you need to segregate user data at a granular level?
- Do you need to encrypt data before storing it in the cloud?
- Are you a cloud vendor that needs to keep multi-tenant data segregated?

If the answer to any of these questions is "yes," then NSE can be combined with NAS or SAN encryption to augment your data protection.

Combine encryption for defense in depth

If you need to segregate access to data as well as make sure that data is protected all of the time, NSE can be combined with network- or fabric-level encryption. NSE can act like a backstop in case an administrator forgets to configure or misconfigures higher level encryption.

Get Exceptional Enterprise Service and Support

Like all of our products, NSE comes with NetApp's world-class service and support infrastructure and longtime industry expertise. We deliver global enterprise-class services, support, and consulting to help you plan, evaluate, and implement your storage security strategy through every phase to maximize your return on investment as your business grows.

Supported Storage Modules

- FAS2040
- FAS3200 series
- FAS6200 series
- DS4243 with 600GB NSE drives

About NetApp

NetApp creates innovative storage and data management solutions that deliver outstanding cost efficiency and accelerate business breakthroughs. Discover our passion for helping companies around the world go further, faster at *www.netapp.com*.

Go further, faster®

NetApp®

www.netapp.com