Datasheet

NetApp Storage Encryption

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

Key Benefits

Gain Full Disk Encryption
SEDs prevent data access until the drive's encryption key is unlocked by an authorized administrator.

Perform Mandatory Data Encryption
NSE and NVMe SEDs are 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.

Enhance Data Confidentiality and Integrity
Use NSE or NVMe SEDs along with NVE and NAE to take advantage of the industry's first double encryption solution using two distinct layers. This combination provides a more robust data encryption solution.

Maintain Storage Efficiencies
By using NSE, NVMe SEDs, NVE, or NAE, you can encrypt your data while maintaining NetApp storage efficiencies such as deduplication and compression.

Satisfy Governance and Compliance Requirements
Use established security best practices to adhere to and support industry regulation and security compliance, including FIPS 140-2 level 2 with NSE.

The NetApp® ONTAP® storage management solution continues to evolve, with security as an integral part of the solution. With NetApp Storage Encryption (NSE), full disk encryption is available using self-encrypting drives (SEDs) that are FIPS 140-2 level 2 certified. In addition, the strength of the portfolio and ONTAP solution continues with the arrival of NVMe SEDs, available in ONTAP 9.6 (not FIPS 140-2 certified); NetApp Volume Encryption (NVE), available in ONTAP 9.1; and NetApp Aggregate Encryption (NAE), available in ONTAP 9.6. NVE and NAE let you encrypt the data at a volume level, making the solution agnostic of the physical drive. In addition, the ability to take advantage of both hardware and software encryption options, providing double encryption at rest, is an industry first.

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 the personally identifiable information, personal healthcare information, and customer information protected within your storage infrastructure becomes a challenge when you repurpose drives, return defective drives, or upgrade 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 the time without affecting everyday operations?

The Solution

NetApp Storage Encryption

NSE uses FIPS 140-2 level 2 SEDs to facilitate compliance and spares return by enabling the protection of data at rest, through AES 256-bit transparent disk encryption. The drives perform all the data encryption operations internally, as depicted in Figure 1, including encryption key generation. To prevent unauthorized access to the data, the storage system must authenticate itself with the drive by using an authentication key that is established the first time the drive is used. This can be done with either the onboard key manager (OKM) or an external key manager.

NSE can use the OKM to set and store the authentication keys for NSE drives. When the system uses an external key manager, the authentication keys are backed up externally using the industry-standard OASIS Key Management Interoperability Protocol (KMIP). With the external key manager, only the storage system, drive, and key manager have access to the key, and the drive cannot be unlocked if it is moved outside the security domain, thus preventing data leakage.

NetApp®

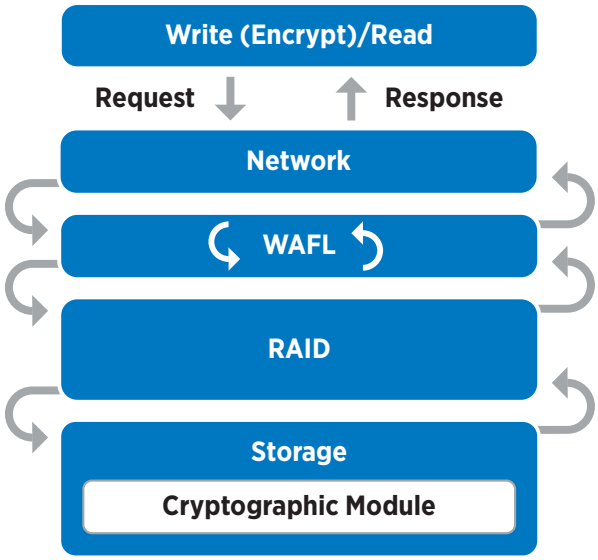

Figure 1) NSE cryptographic function.

Do I Need NSE?

Here are some questions to ask yourself:

- Must physical media be encrypted?
- Do I have any physical drive encryption requirements—for example, tamper evidence solutions?
- Must root aggregate volumes and storage virtual machine volumes be encrypted?
- Do I require ubiquitous disk encryption of all data?

If the answer to any of these questions is yes, then NSE is a viable solution.

Combine encryption for double encryption (layered defense)

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

NSE Supported Storage Architectures

- NetApp AFF A-Series
- NetApp FAS9000 series
- NetApp FAS8200 series
- NetApp FAS2650 series
- NetApp FAS2620 series

Contact your account team to find out more about how the NSE solution can solidify your organization's needs. The following table lists some of the basics of NSE.

Entire disk encrypted
Hardware based
AES 256 encryption
NSE SEDs required
Onboard or external key management for the authentication key
FIPS 140-2 validated when used with external key manager; FIPS level depends on key manager use and implementation
All drives (including HA pairing) must be NSE drives; no mixing NSE and non-NSE drives

Resources

- NetApp Storage Encryption, NVMe Self-Encrypting Drives, NetApp Volume Encryption, and NetApp Aggregate Encryption datasheet
- NetApp Volume Encryption and NetApp Aggregate Encryption datasheet

About NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. For more information, visit www.netapp.com. #DataDriven