Datasheet

NetApp Storage Encryption (NSE) and NetApp Volume Encryption (NVE)

Two encryption-at-rest solutions

Key Benefits

Enhance Data Confidentiality and Integrity with the Industry-First Double Encryption Solution Using Two Distinct Layers
Use both NSE and NVE to provide a more robust data encryption solution.

Maintain Secure Posture Regardless of Physical Media
With NVE, encrypting at the volume level allows the encryption capability to exist independently of the physical media: solid-state drives (SSDs), All Flash FAS (AFF), or even SEDs.

Maintain Storage Efficiencies
The use of NSE and/or NVE allows the ability to 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 the advent of NSE, full disk encryption is available using self-encrypting drives (SEDs). In addition, the strength of the portfolio and ONTAP solution continues with the arrival of NVE (available in ONTAP 9.1), which provides the ability to encrypt the data at a volume level, allowing the solution to be agnostic of the physical drive. Also, the ability to leverage both options, providing double encryption at rest, is an industry first.

To learn more about hardening the ONTAP 9 solution, see TR-4569: ONTAP 9 Security Hardening Guide.

The Challenge of Options

Each day, new requirements and regulations are released or updated to address an organization's ability to mitigate risk and gaps in the infrastructure when repurposing drives, returning defective drives, or upgrading to larger drives by selling or trading them in. As administrators and operators of data and information, storage engineers are expected to manage and maintain data in a secure manner throughout its lifecycle. NSE and NVE offer key options to solve the challenge of making sure that all of your data is encrypted, all the time, and without affecting daily operations. Yet which option is most suitable for your deployment? NSE? NVE?

The Solution

This datasheet provides an overview of the NSE and NVE solutions and their functions. A clear understanding of the essential components and details that make up the NSE and NVE solutions is vital for an organization to make sure it institutes the most effective solution for its data encryption needs.

NetApp®

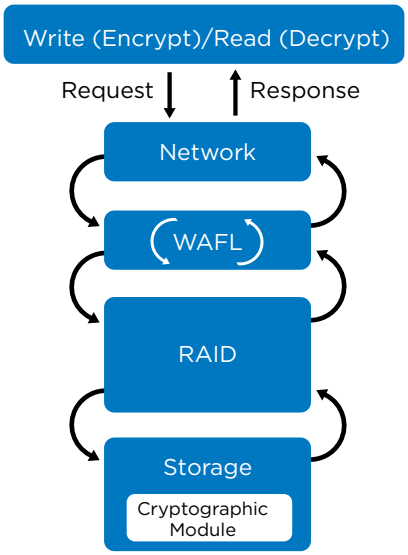

Figure 1) NSE cryptographic function.

NetApp Storage Encryption (NSE)

NSE is configured to use FIPS 140-2 level 2 self-encrypting drives 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 of 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 using an authentication key that is established the first time the drive is used.

NetApp Volume Encryption (NVE)

NVE is a software-based, data-at-rest encryption solution available starting with NetApp ONTAP 9.1 management software. Starting with ONTAP 9.2, NVE is FIPS 140-2 compliant. NVE allows ONTAP to encrypt data (using AES 256-bit encryption) per volume for granularity. Data can also be stored on disk without self-encrypting drives (SEDs). NVE enables you to use storage efficiency features that would be lost with encryption at the application layer. Storage efficiencies are maintained because the data comes in from the network through NetApp WAFL® (Write Anywhere File Layout) to the RAID layer, which determines whether the data should be encrypted. If the data should be encrypted, it is sent to the cryptographic module (CryptoMod), which is FIPS 140-2 level 1 validated. The CryptoMod encrypts the data and sends it back to the RAID layer, and the encrypted data is sent to disk. With the NVE solution, the data is already encrypted on the way to the disk. Reads follow the reverse path. In summary, the data leaves the disk encrypted, is sent to RAID, is decrypted by the CryptoMod, and is then sent up the rest of the stack.

Key Management

External key management

The NSE and NVE solutions can use either external or onboard key management. In the external key management solution, the NSE 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. NVE volume encryption keys are also stored on the external key manager. If the controller and disks are moved without access to the external key manager, the NVE volumes won't be accessible and cannot be decrypted.

Onboard key management (OKM)

Both NSE and NVE use the onboard key management solution. When using the OKM, NVE is composed of a software CryptoMod, encryption keys, and an onboard key manager. NVE uses a unique XTS-AES 256 data encryption key, which is generated per volume. The encryption keys are stored within the onboard key manager, which keeps track of all the encryption keys used by ONTAP. The keys used for a data volume are unique to that data volume in that cluster. The keys are generated when the encrypted volume is created. ONTAP does not pregenerate or reuse keys. These keys are never displayed in plain text and are stored and protected by the onboard key manager. NSE uses the OKM to set the authentication keys for NSE drives.

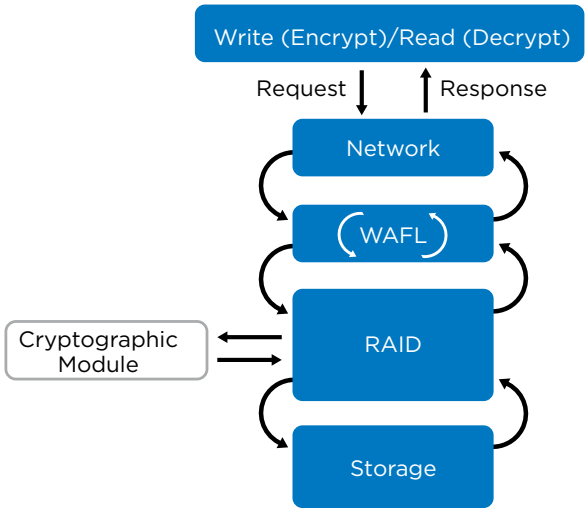

Figure 2) NVE cryptographic function.

Do I Need NSE?

Some questions to ask yourself

- Must physical media be encrypted?
- Do I have any physical drive encryption requirements—for example, tamper evidence solutions?

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

Do I Need NVE?

Some questions to ask yourself

- Do your physical media needs exceed the capacity of self-encrypting drives?
- Are you looking for a software-based at-rest encryption method?
- Are you looking for granularity in terms of what data is to be encrypted?

If the answer to any of these questions is yes, then NVE 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.

Supported Storage Architectures

NSE

- NetApp All Flash FAS (AFF) A-Series
- NetApp FAS9000 series
- NetApp FAS8200 series
- NetApp FAS2650 series
- NetApp FAS2620 series

NVE

- NVE is supported beginning in ONTAP 9.1 and is agnostic to the physical drives being used.

Contact your account team to find out more about how the NSE and NVE solutions can solidify your organization's needs.

To help you understand some of the basics, Table 1 compares NSE and NVE.

Table 1) NSE and NVE comparison.

NSE	NVE
Entire disk encrypted	Encrypts at volume level
Hardware based	Software based
AES 256 encryption	XTS-AES 256 encryption
NSE SEDs required	No need for SEDs
Onboard or external key management	Onboard or external key management
FIPS 140-2 level 2 validated when used with external key manager; FIPS level depends on key manager use and implementation	FIPS 140-2 level 1 validated for the CryptoMod
All drives (including HA pairing) must be NSE drives; no mixing NSE and non-NSE drives	

Remember that for double encryption, NSE and NVE can be used together.

Resources

NetApp Storage Encryption Datasheet
NetApp Volume 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