Datasheet

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

Four encryption-at-rest solutions

Key Benefits

Enhance Data Confidentiality and Integrity with the Industry-First Double Encryption Solution Using Two Distinct Layers
Use both software (NVE or NAE) and hardware (NSE or NVMe SED) to provide a more robust data encryption solution.

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

Maintain Storage Efficiencies
NSE, NVMe SEDs, NVE, and NAE allow you 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 NetApp Storage Encryption (NSE), full disk encryption is available with FIPS 140-2 level 2 self-encrypting drives (SEDs). Full disk encryption is also available for NVMe SEDs that do not have FIPS 140-2 certification. In addition, the strength of the portfolio and ONTAP solution continues with NetApp Volume Encryption (NVE, available in ONTAP 9.1) and NetApp Aggregate Encryption (NAE, available in ONTAP 9.6). These technologies encrypt data at the volume and aggregate level, respectively, making the solution agnostic of the physical drive. By using both software (NVE or NAE) and hardware (NSE or NVMe SED), you can achieve double encryption at rest, which 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, NVMe SEDs, NVE, and NAE 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? Software-based data-at-rest encryption (NVE, NAE)? Hardware-based data-at-rest encryption (NSE, NVMe SEDs)?

The Solution

This datasheet provides an overview of the NSE, NVMe SED, NVE, and NAE solutions and their functions. A clear understanding of the essential components and details that make up these solutions is vital so that an organization can institute the most effective solution for its data encryption needs.

NetApp®

NetApp Storage Encryption

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.

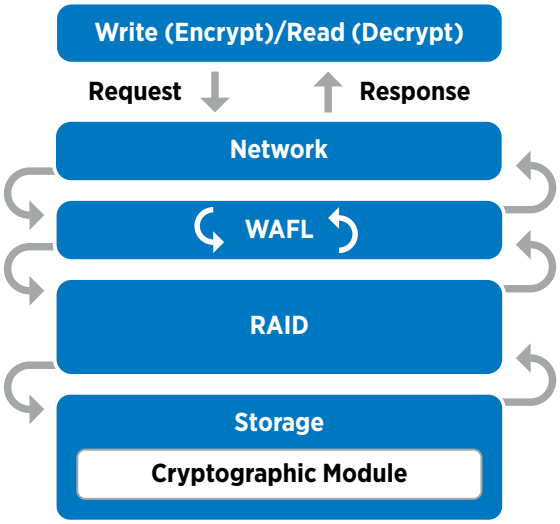

Figure 1) NSE cryptographic function.

NVMe Self Encrypting Drives

NVMe SEDs do not carry the FIPS 140-2 certification. However, they are still configured to use self-encryption to facilitate spares return: They use AES 256-bit transparent disk encryption to protect data at rest. The disks 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 disk using an authentication key that is established the first time the disk is used.

NetApp Volume Encryption and NetApp Aggregate Encryption

NVE is a software-based, data-at-rest encryption solution available starting with ONTAP 9.1, and it has been FIPS 140-2 compliant since ONTAP 9.2. NVE allows ONTAP to encrypt data for each volume for granularity. NAE, available with ONTAP 9.6, is an outgrowth of NVE; it allows ONTAP to encrypt data for each volume, and the volumes can share keys across the aggregate. Both NVE and NAE use AES 256-bit encryption. Data can also be stored on disk without SEDs.

NVE and NAE enable 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® to the RAID layer, which determines whether the data should be encrypted. For greater storage efficiency, you can use aggregate deduplication with NAE. NVE volumes and NAE volumes can coexist on the same NAE aggregate. NAE aggregates do not support unencrypted volumes.

Here's how the process works: If 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. The encrypted data is then sent to disk. So, with the combination of NVE and NAE, the data is already encrypted on the way to the disk. Reads follow the reverse path. In other words, 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. This process is outlined in Figure 3.

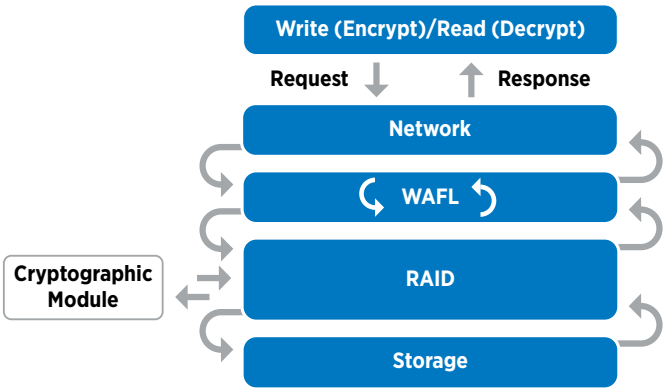

Figure 3) NVE and NAE cryptographic function.

Key Management

The NSE, NVMe SED, NVE, and NAE solutions can use either external or onboard key management.

External key management

In external key management, the NSE and NVMe SED authentication key is backed up to an external key manager by 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 the security domain, thus preventing data leakage. The external key manager also stores NVE volume encryption keys and NAE aggregate encryption keys. If the controller and disks are moved and no longer have access to the external key manager, the NVE and NAE volumes won't be accessible and cannot be decrypted.

Onboard key management

The onboard key manager (OKM) keeps track of all the encryption keys used by ONTAP. NSE and NVMe SEDs use the OKM to set the authentication keys for NSE or NVMe SEDs.

When using the OKM, the combined NVE and NAE solution is composed of a software CryptoMod, encryption keys, and an OKM. For each volume, NVE uses a unique XTS-AES 256 data encryption key, which the OKM stores. The key used for a data volume is unique to that data volume in that cluster and is generated when the encrypted volume is created. Similarly, an NAE volume uses unique XTS-AES 256 data encryption keys per aggregate, which the OKM also stores. NAE keys are generated when the encrypted aggregate is created. ONTAP does not pregenerate or reuse keys. ONTAP does not pregenerate keys, reuse them, or display them in plain text; they are stored and protected by the OKM.

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 (FIPS 140-2)?

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

Do I Need an NVMe SED?

Some questions to ask yourself

- Must physical media be encrypted?
- Am I able to encrypt the physical media without the requirement for tamper evidence solutions like FIPS 140-2?

If the answer to both of these questions is yes, then NVMe SEDs are a viable solution.

Do I Need NVE and NAE?

Some questions to ask yourself

- Do my physical media needs exceed the capacity of NSE or NVMe SED?
- Do I want a software-based at-rest encryption method?
- Do I want granularity in terms of what data is to be encrypted?

If the answer to any of these questions is yes, then NVE and NAE are viable solutions.

Combine encryption for double encryption (layered defense)

If you need to segregate access to data and make sure that data is protected all the time, NSE or NVMe SEDs can be combined with network- or fabric-level encryption. NSE and NVMe SED 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 or NVMe SEDs with NVE and NAE.

Supported Storage Architectures

NSE

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

NVE and NAE

- NVE is supported beginning in ONTAP 9.1 and is agnostic to the physical drives being used.
- NAE is supported beginning in ONTAP 9.6 and is also agnostic to the physical drives being used.

Contact your account team to find out more about how the NSE, NVMe SED, NVE, and NAE solutions can satisfy your organization's needs.

To help you understand some of the basics, Table 1 compares NSE, NVMe SED, and the combined NVE and NAE solution.

NSE	NVE AND NAE	NVMe SED
Entire disk encrypted	Encryption at volume level	Entire disk encrypted
Hardware based	Software based	Hardware based
AES 256 encryption	XTS-AES 256 encryption	AES 256 encryption
NSE SEDs required	No need for SEDs	NVMe SEDs required
Onboard or external key management	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	No FIPS 140-2 certifications
All drives (including HA pairing) must be NSE drives; you cannot mix NSE and non-NSE drives		You can mix NVMe SSDs and NVMe SEDs, but not NSE drives

Table 1) NSE, NVE and NAE, and NVMe SED comparison.

Remember that for double encryption, software (NVE or NAE) and hardware (NSE or NVMe SEDs) can be used together.

Resources

NetApp Storage Encryption datasheet

NetApp Volume Encryption and NetApp Aggregate Encryption datasheet

About NetApp

Leading organizations worldwide count on NetApp for software, systems and services to manage and store their data. Customers value our teamwork, expertise and passion for helping them succeed now and into the future.

www.netapp.com