DATASHEET

NETAPP STORAGE ENCRYPTION AND NETAPP VOLUME ENCRYPTION

Two encryption-at-rest solutions

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. Risks and gaps can occur when repurposing drives, returning defective drives, or upgrading to larger drives by selling or trading them in. Storage engineers are expected to manage and maintain data in a secure manner throughout its lifecycle.

The NetApp® ONTAP® storage management solution continues to evolve, and security is an integral part of the solution. NetApp offers two complementary encryption solutions designed to secure data at rest with distinct approaches suitable for different deployment needs: NetApp® Storage Encryption (NSE) and NetApp Volume Encryption (NVE). These solutions provide robust data protection while maintaining storage efficiency and compliance with industry standards.

NSE and NVE offer key options for making sure that all your data is always encrypted, without affecting daily operations. However, which solution is most suitable for your deployment—NSE or NVE?

The solution

With NSE, full-disk encryption is available using self-encrypting drives (SEDs), and with NVE, data can be encrypted at a volume level, allowing a solution to be physical drive–agnostic. The use of both options, which provides double encryption at rest, is an industry first.

This datasheet provides an overview of the NSE and NVE solutions and their functions. With a clear understanding of the essential components of these solutions, your organization can choose the right solution for its data encryption needs.

NetApp Volume Encryption

NVE is a software-based, data-at-rest encryption solution available starting with ONTAP 9.1, and has been FIPS 140-3 compliant since 9.15.1. Using AES 256-bit encryption, NVE allows ONTAP to encrypt data for each volume for granularity. Data can also be stored on disk without SEDs. Figure 2 depicts data encryption with NVE.

NetApp Storage Encryption

NSE is configured to use either FIPS 140-2 or FIPS 140-3 level 2 SEDs to facilitate compliance and spares return by enabling the protection of data at rest. This is accomplished using either AES-256 or XTS-AES-256 transparent disk encryption. The type of encryption used depends on the drive model and the drive's FIPS certificate security policy.

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 using an authentication key that is established the first time the drive is used.

(For more information on determining a drive's FIPS certification, see the KB article How to determine FIPS 140-2 or 140-3 certification number for encrypting drives.)

Note: NSE and NVE use AES-256 bit encryption which is a quantum resistant algorithm that protects from harvest now and decrypt later attacks.

Enhance data confidentiality and integrity with the first double-encryption solution in the industry to use two distinct layers.
Use both NSE and NVE to provide a more robust data encryption solution.

Maintain secure posture regardless of physical media.
Using encryption at the volume level allows the encryption capability to exist independently of the physical media (SSDs, NetApp AFF systems, or even SEDs).

Maintain storage efficiencies.
The use of NSE and/or NVE allows you to encrypt your data while maintaining NetApp storage efficiencies such as deduplication and compression.

Satisfy governance and compliance requirements.
Leverage established security best practices to adhere to and support industry regulation and security compliance, including FIPS140-3 level 2 and FIPS 140-2 level 2, depending on the SED drives used.

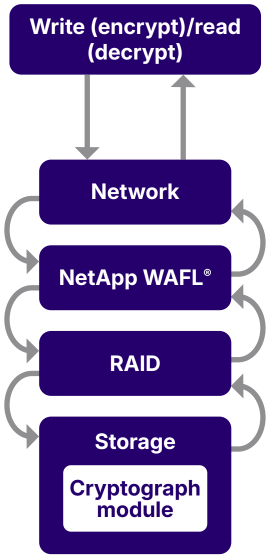

Figure 1:
Cryptographic function

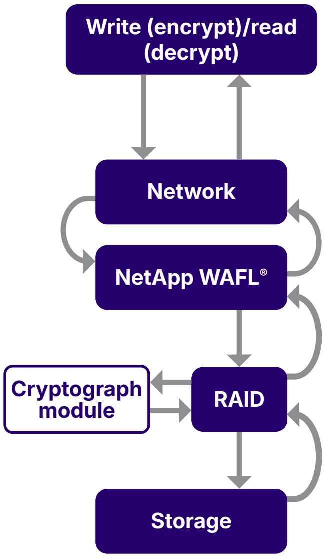

Figure 2:
NVE cryptographic function

Key management

External key management

The NSE solution can use external or onboard key management. In an external key management solution, 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.

Onboard key management

Both NSE and NVE can use onboard or external key management. NVE is composed of a software cryptographic module, encryption keys, and an onboard key manager (OKM). NVE leverages a unique XTS-AES-256 data encryption key, generated for each volume and stored in the OKM, 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. ONTAP does not pregenerate or reuse keys; they are generated when the encrypted volume is created. The keys are never displayed in plain text and are protected by the OKM.

For more information about how the OKM works and how keys are managed and secured, see the following documents, available from your NetApp representative:

“Overview of the ONTAP Onboard Key Manager (OKM)”
- TR-5014-0625

“NDA Addendum: ONTAP Onboard Key Manager (OKM)”
- TR-5013-0625

If you need to segregate access to data and make sure that data is protected all the time, NSE can be combined with network-level or fabric-level encryption. NSE can act like a backstop in case an administrator forgets to configure or misconfigures higher-level encryption. You can use any existing disk with NVE, including NSE drives, for two distinct layers of encryption.

Supported storage architectures

NSE

NetApp ONTAP 9 FAS and AFF systems.

NVE

NVE is supported beginning with ONTAP 9.1 and is drive-agnostic.

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 the basics, *Table 1* compares NSE and NVE.

NetApp Storage Encryption	NetApp Volume Encryption
Encrypts entire disk	Encrypts at the volume level
Hardware based	Software based
AES-256 encryption	XTS-AES-256 encryption
Requires SEDs (NSE drives)	No need for SEDs
Onboard or external key management	Onboard or external key management
FIPS 140-2 and FIPS 140-3 level 2 validated, depending on the model of SED drives	FIPS 140-3 level 1 validated
All drives (including HA pairing) must be NSE drives. No mixing NSE and non-NSE drives.	Software-based encryption is drive-agnostic

Table 1: Comparison of NSE and NVE

Do I need NSE?

Some questions to ask yourself:

Must physical media be encrypted?

Do I have any physical drive encryption requirements?

For example, do I need tamper-evident 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 my physical media needs exceed the capacity of SEDs?

Am I a cloud vendor that needs to keep multitenant data segregated?

Am I looking for a software-based, at-rest encryption method?

Am I 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.

Contact Us

About NetApp
For more than three decades, NetApp has helped the world’s leading organizations navigate change – from the rise of enterprise storage to the intelligent era defined by data and AI. Today, NetApp is the Intelligent Data Infrastructure company, helping customers turn data into a catalyst for innovation, resilience, and growth. At the heart of that infrastructure is the NetApp data platform – the unified, enterprise-grade, intelligent foundation that connects, protects, and activates data across every cloud, workload, and environment. Built on the proven power of NetApp ONTAP, our leading data management software and OS, and enhanced by automation through the AI Data Engine and AFX, it delivers observability, resilience, and intelligence at scale. Disaggregated by design, the NetApp data platform separates storage, services, and control so enterprises can modernize faster, scale efficiently, and innovate without lock-in. As the only enterprise storage platform natively embedded in the world’s largest clouds, it gives organizations the freedom to run any workload anywhere with consistent performance, governance, and protection. With NetApp, data is always ready – ready to defend against threats, ready to power AI, and ready to drive the next breakthrough. That’s why the world’s most forward-thinking enterprises trust NetApp to turn intelligence into advantage.

Learn more at **www.netapp.com** or follow us on **X**, **LinkedIn**, **Facebook**, and **Instagram.**