Solution Brief

Quantum-Ready Data-at-Rest Encryption by NetApp

Securing data in the age of quantum computing

Key Benefits

Quantum-Ready Encryption

Designed to re-encrypt existing data and easily incorporate updates to add new quantum-resistant encryption algorithms.

Encryption for TOP SECRET Documents

Provides AES-256 encryption to support the current NSA recommendation for protecting against quantum attacks.

Industry-First Encryption Solution: Native, FIPS Validated 2-layers

Two distinct layers of software- and hardware-based encryption as required by the NSA's Commercial Solutions for Classified Program.

Secure and Protect Efficiently

Preserve storage efficiencies while encrypting data.

- Deduplication
- Compression
- Compaction

The Quantum Computing Challenge

Certain forms of encryption will no longer be secure because of quantum computing.

Validated and tested cryptography relies on the premise that cracking the encryption scheme is computationally hard and extremely time consuming using existing computing. However, new computational methods, labeled quantum computing, threaten some encryption schemes. These new methods allow the use of unique algorithms, which reduce the time required to crack some encryption schemes. When quantum computing is prevalent, systems and algorithms that were once believed to be secure will be at risk for being compromised. Security-savvy organizations are already preparing to migrate to stronger, quantum-resistant encryption.

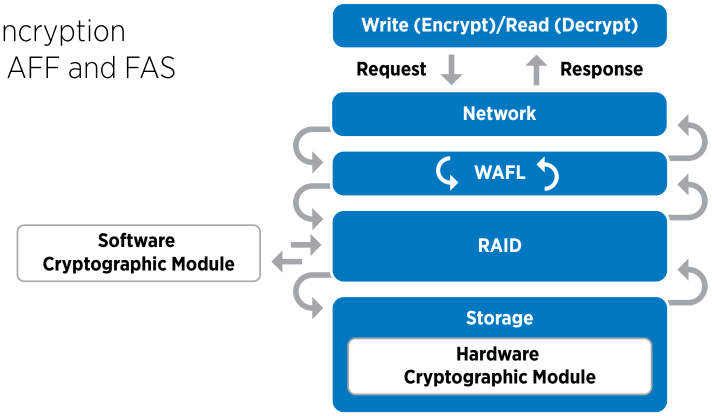
Preparing for Quantum Resistant Encryption

NetApp provides layered, quantum-ready encryption natively.

The NSA has published the Commercial National Security Algorithm Suite in which they've listed AES-256 as the recommended algorithm and key length until the quantum-resistant encryption algorithms have been defined (CSNA Suite and Quantum Computing FAQ). Furthermore as part of the Commercial Solutions for Classified Program, the NSA recommends a layered encryption approach with a software and hardware layer.

NetApp Volume Encryption (NVE), a key feature in NetApp ONTAP data management software, provides FIPS 140-2 validated, AES-256 encryption via a software cryptographic module. NetApp Storage Encryption (NSE) utilizes self-encrypting drives to deliver FIPS 140-2 validated, AES-256 encryption for AFF all-flash and FAS hybrid-flash systems. These two distinct encryption technologies can be combined together to provide a native, layered encryption solution that provides encryption redundancy and additional security: if one layer is breached, the second layer is still securing the data.

Two-layer encryption solution for AFF and FAS


Write (Encrypt)/Read (Decrypt)
Request
Response
Network
WAFL
RAID
Software Cryptographic Module
Storage
Hardware Cryptographic Module

Future-Proof: Quantum Ready Encryption

With the NetApp software encryption module, future quantum-resistant algorithms can be added simply.

At the heart of NVE is a software cryptographic module that can encrypt, decrypt, and re-encrypt any data residing today on a NetApp ONTAP system, AFF or FAS. This simple, non-disruptive capability is currently available in NVE and paves the way for a seamless transition to quantum-resistant encryption in the future. Existing data can be re-encrypted with the latest, greatest algorithms as they become validated by government agencies such as the National Institute of Standards and Technology (NIST).

To learn more NetApp security features, please read Security Features in ONTAP 9 Data Sheet.

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