Qlogic Enhances Fibre Channel Security with Post-Quantum Cryptography

- Marvell® QLogic® StorCryption® supports Zero Trust Architectures
  - Silicon Root of Trust
  - HBA attestation
  - Autonomous Encrypted Data in Flight
  - Post-Quantum Cryptography
- QLogic HBAs enable
  - Compliance with NIS2, DORA, and other government mandates
  - Simplified security deployment in existing FC SANs
  - Defense in depth security for mission critical data
  - FIPS 140-3 security
  - Wire speed end-to-end encryption

Fibre Channel (FC) SANs are deployed in over 90% of Fortune 1000 customer data centers that run mission-critical storage workloads. With ever increasing threat vectors both inside and outside the data center, a compromised customer dataset can quickly result in a torrent of lost business data, eroded trust, significant penalties, and potential lawsuits. There are potential vulnerabilities at every point in the enterprise infrastructure which requires data to be secured not only when it leaves the data center or is exposed to the internet, but every time it leaves a server or the storage media.

QLogic Extends SAN Security with Zero Trust Architecture

Like any network that transacts data, Fibre Channel SANs face new and renewed threats. This is driving the industry to do more to secure Fibre Channel. The Fibre Channel protocol and a majority of Fibre Channel devices -- from HBAs to switches and storage devices, implement various security mechanisms ranging from access control via zoning, LUN Masking to physical segregation of storage and local area networks.

However, the increased risk of today's multi-tenancy environments that share Fibre Channel SAN resources across an increasing amount of host applications combined with increasing occurrences of insider attacks, data breaches, and other persistent cyberattacks drive the need for additional layers of protection. In addition, government compliance regulations including EO14028, NIS2, DORA, HIPAA, GDPR and ISO27001 A.10 increasingly require that transmission and storage of customer data be secured-via authenticated hardware (silicon root of trust & device attestation) and data encryption (FC-SP) and now with PQC algorithms, all in a Zero Trust Architecture.

The level of security that will be required for Fibre Channel SANs is more than just encrypting storage media, as this only secures data against physical theft from the data center and does not protect against vulnerabilities while the data is in transit between host and storage media. During normal operations, data leaves shared storage devices unencrypted, which may pose a security risk. Adding defense in depth to the Fibre Channel SANs beyond traditional host-based and network-based data protection is prudent and provides additional protection of mission-critical data that frequently traverse the Fibre Channel storage area network to address the emerging threat landscape.

It's Now a Post-Quantum World

Due to advancements in computing, there is concern that public key systems could someday be compromised by quantum computers. This has resulted in a critical requirement to protect systems from future deployment of cryptographically relevant quantum computers (CRQC). The Commercial National Security Algorithm Suite (CNSA) 2.0 is a set of cryptographic algorithms standardized by the National Security Agency, and serves as the cryptographic base to protect US National Security Systems information up to the top secret level.

Marvell introduced StorCryption™ in 2019 and has enhanced the protocols, algorithms, and methods to extend our years of deployments and decades of proven security of storage networking technologies to the next level:

- Post-Quantum Cryptography (PQC)
- Silicon Root of Trust
- HBA host attestation
- Autonomous Encryption of Data in flight (EDiF)

Compliance Requires StorCryption to Secure All Data Paths

The US and EU governments have implemented "Zero Trust" mandates for equipment and operational resiliency with EO 14028 for US government, Network and Information Security (NIS2) for EU businesses, and Digital Operations Resilience Act (DORA) for EU financial markets. To comply, OEMs must secure equipment with silicon Root of Trust & SPDM, and data with FC-SP. This includes fortifying the back-end networks (e.g. Fibre Channel) along with the front-end networks.

StorCryption Enhances Data Center Security with Post Quantum Crypto (PQC)

Marvell® QLogic® latest generation of Adapters with StorCryption are fortified with CNSA 2.0 PQC security strength:

Security Application	Security Function	CNSA 2.0 Algorithm
Silicon RoT	FW Signing	LMS
SPDM	Endpoint Attestation	ML-DSA-87
FC-SP-3	Endpoint Authentication	ML-DSA-87
	Key Establishment	ML-KEM-1024
	Encrypted Communications	AES-256

- Marvell QLogic adapters' architecture includes Marvell's CNSA 2.0 firmware signing public key and Fibre Channel firmware appended with a CNSA 2.0 signature to fortify Silicon Root of Trust
- Marvell QLogic adapters' architecture includes X.509 certificates with Marvell's CNSA 2.0 keys & signatures to attest to the latest host servers with BMC support for SPDM
  - Marvell QLogic adapters' architecture also include X.509 certificates with Marvell's CNSA 1.0 keys & signatures to attest to servers that still support SPDM
- Marvell QLogic adapters' architecture autonomously extends Marvell's CNSA 1.0 & 2.0 X.509 certificates to negotiate FC-SP-3 security with compatible endpoints, to seamlessly and transparently authenticate endpoints, create session keys, and transmit & receive encrypted FC SAN data

QLogic Fibre Channel Adapters with Silicon Root of Trust Protects Against Malware

Marvell QLogic Adapters incorporate Silicon Root of Trust (RoT) technology that prevents malicious firmware from hijacking the Fibre Channel adapter. This defends against unauthorized software accesses and changes to configuration of storage networking components. Marvell QLogic adapters contain Marvell's CNSA 2.0 public key and receive Marvell Fibre Channel firmware appended with a CNSA 2.0 signature. qAt each boot or FW update, Marvell QLogic adapters perform a CNSA 2.0 verification operation using the Marvell public key to authenticate the signed firmware. Marvell's silicon contain an embedded hardware security (eHSM) module that creates a FIPS 140-3 boundary around all keys, including the FW verification key.

Hardware-based security provides a "chain of trust" rooted in silicon that extends the security & trust of the Fibre Channel Host Bus Adapter (HBA) to the storage area network (SAN). To harden hardware-based attack surfaces against firmware exploits, servers must secure their own firmware, along with the firmware of all adapters. This enables a chain of trust that extends from the motherboard across all adapters providing a cohesive security architecture that protects the server against hardware-based threat vectors. This in turn provides a trusted foundation for additional layers of security, such as secure boot.

Here are some of the benefits Marvell QLogic FC HBAs deliver value to an enterprise and/or data center:

- Security technologies rooted in "immutable" silicon-based hardware to harden platform attack surfaces
  - Critical as attackers are increasingly launching sophisticated attacks on hardware
- Silicon/hardware embedded keys ensure only validated firmware executes on the FC HBA
  - Prevents malicious firmware from hijacking the Fibre Channel adapter
  - Delivers additional layers of Defense in Depth
- Ensures both integrity and authenticity during adapter firmware updates
  - Protects firmware updates in critical environments and at remote locations
- Eliminates threat vectors and protects servers by leveraging quantum-resistant cryptography

Security Protocol and Data Model (SPDM) HBA Attestation

Marvell QLogic HBAs support Security Protocol and Data Model (SPDM) Specification which enables servers to cryptographically verify the identity of the HBA before it can access data across the PCIe bus. To ensure secure communication, at every server boot, Marvell QLogic SPDM-enabled HBAs:

- Negotiate with host motherboard baseboard management controller (BMC) over the PCIe bus how they will authenticate each other's identities.
- Marvell QLogic SPDM-enabled HBAs attest themselves by signing measurements (device configurations) to confirm its identity to the server BMC.
- SPDM can also be used to create an encrypted channel for secure communications and subsequent data (PCIe IDE) to safeguard data sent & received across the PCIe bus from eavesdroppers.

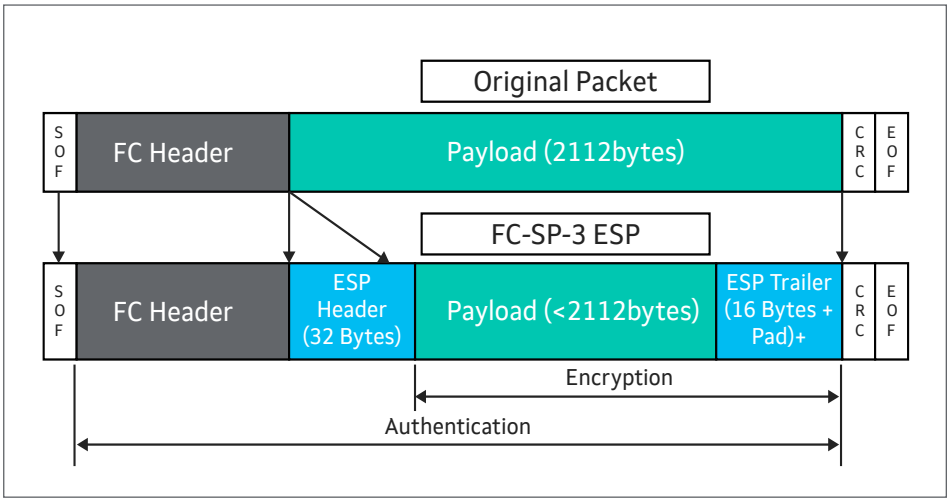
To simplify deployments into servers during the transition from CNSA 1.0 to CNSA 2.0, Marvell QLogic HBAs support both ECDSA 384 (CNSA 1.0) and ML-DSA-87 (CNSA 2.0).

Second Generation Autonomous Fibre Channel In-Flight Encryption with PQC-Enabled StorCryption

Marvell StorCryption supports Fibre Channel Security Protocol (FC-SP-3), a standard that defines security mechanisms for FCP (Fibre Channel Protocol), FC-NVMe (NVMe over Fibre Channel) and FICON (Fibre Connection), developed by the ANSI T11 Technical Committee of the International Committee on Information Technology Standards (INCITS). Marvell StorCryption supports a security framework which includes extending:

- IKEv2 authentication to incorporate ML-DSA-87
- Cryptographically secure key exchange to incorporate ML-KEM-1024
- Cryptographically secure communication utilizing AES-GCM-256 between Fibre Channel devices.

Marvell StorCryption implements its eHSM to autonomously, seamlessly, transparently, and securely authenticate endpoints, generate random session keys, and protect data in flight within a Fibre Channel SAN. Furthermore, Marvell StorCryption can operate in conjunction with switch-based ISL encryption, as well as encrypted data at rest (EDAR), but without requiring key vaults or lifecycle management. StorCryption eliminates the need for server-based encryption solutions that consume host CPU cycles (e.g. file system, database, disk encryption software, etc.), while allowing storage arrays to continue featuring value-added services, such as data reduction, deduplication, etc., along with security of data at rest.



Marvell StorCryption supports FC-SP-3's ESP security protocol for Fibre Channel frames that provides origin authentication, integrity, anti-replay protection, and confidentiality. Marvell StorCryption has adopted the IKEv2 protocol (used in IPsec) to autonomously provide authentication of Fibre Channel entities and setup session-based security associations using PQC algorithms. Within this framework, a StorCryption-enabled device can autonomously verify the identity of another Fibre Channel device and establish shared secrets that will be used to negotiate security associations for security protocols to encrypt Fibre Channel frames in flight, all while maintaining end-to-end data protection.

Protections Provided by the Fibre Channel Security Protocol

Marvell StorCryption enables the following additional protections for Fibre Channel SANs:

- **Origin authentication** - verification that the traffic came from a given endpoint.
- **Integrity assurance** – assurance that the data transmitted was not tampered with before being received at the other end.
- **Anti-replay protection** – avoids a network attack in which a valid data transmission is maliciously or fraudulently repeated.
- **Confidentiality** – only the sender and receiver have access to the data contents of the frame.

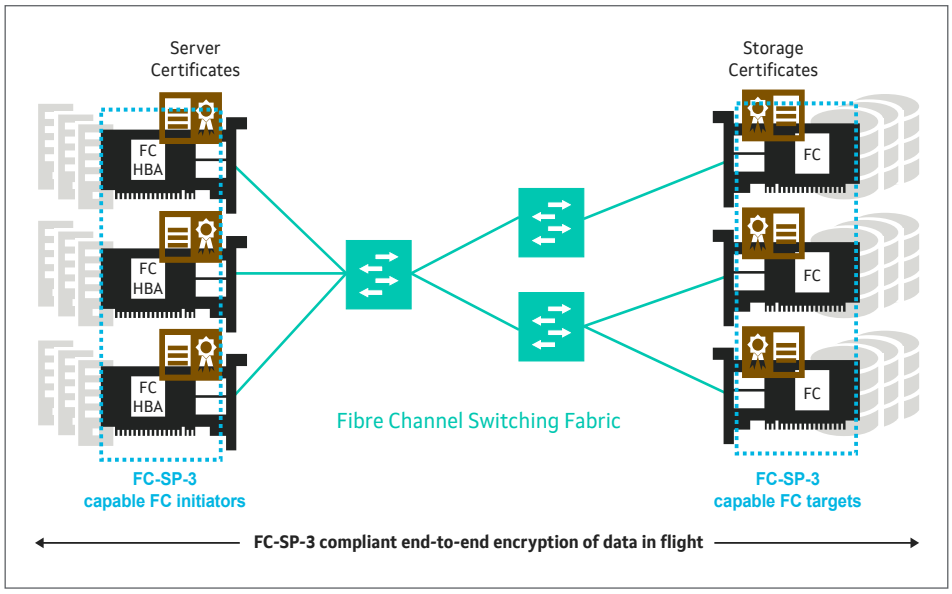
Ecosystem and Market Dynamics

Increased occurrences of insider attacks, theft of data while in transit, as well as government compliance regulations have driven Marvell StorCryption to adopt Zero Trust architectures and productize end-to-end Fibre Channel SAN encryption with endpoint authentication, along with silicon Root of Trust and server device attestation. This new generation of security implementations will work with existing SAN switch infrastructure to thwart the dangers of "harvest now and decrypt later" threat models. For example, the FC-SP-3 specification defines encrypted payloads with Fibre Channel

headers sent in clear text, enabling encryption of data in flight to function with existing SAN switching.

Marvell StorCryption's Encryption of Data in Flight seamlessly secures the entire SAN which is critical not only between data centers, but also within data centers. Many Fibre Channel switches implement encryption for the data traffic that flows between Inter-Switch Links (link encryption), however Marvell StorCryption autonomously, seamlessly, and transparently enables an end-to-end solution between host HBAs and storage devices without requiring extra hardware to manage endpoint certificates.

A true secure SAN is one with end-to-end encryption, endpoint authentication, device attestation and silicon Root of Trust.



For more information, contact storcryption@marvell.com