Solution Brief

Emulex® SecureHBA Delivers the Industry's First Autonomous In-Flight Encryption with Post-Quantum Cryptography for EMEA

Challenge

Organizations are evaluating better data security solutions to solve a range of problems:

- Prevent data breaches such as unauthorized access to sensitive data
- Compliance with current and upcoming government mandates and guidelines
- Avoid financial loss from ransomware and cyber attacks
- Protect intellectual property and trade secrets
- Maintain customer trust by demonstrating that the organization takes data security seriously

Opportunity

This solution brief discusses how the Emulex® SecureHBA—the most secure and cost-effective data storage solution that utilizes existing infrastructure—delivers the following:

- Compliance with government regulations and guidelines
- Easy-to-deploy encryption at no additional cost
- Secures sensitive data with current state-of-art and post-quantum cryptography
- Prevents malicious attacks on storage adapter firmware
- Timely detection and recovery from ransomware attacks
- Ensures the authenticity of storage adapter verification by the host

The Data Security Challenge

In today's digital landscape, organizations are increasingly dependent on vast amounts of sensitive data, including personal, financial, and intellectual property. However, the growing frequency and sophistication of cyber attacks, data breaches, and unauthorized access have made protecting this data more challenging than ever. Data breaches not only result in financial losses but also undermine customer trust, adherence with governmental regulations, and the overall integrity of business operations.

Current data protection methods, firewalls, and access controls are often insufficient in addressing emerging threats. There is a pressing need for advanced, scalable, and dynamic data security solutions that can effectively mitigate risk, protect sensitive information, and ensure compliance with evolving privacy regulations.

The powerful new quantum computers on the horizon are also worrisome, as they will add significant new threats on top of increasing baseline risks. Cybersecurity experts fear that quantum computers will be able to crack cryptographic algorithms that have long resisted cyber attack by traditional computers. The practice of stealing encrypted data now and storing it until it can be decrypted later with a quantum computer is already a very real concern. This kind of attack is known as the *harvest now and decrypt later* threat model.

Government Mandates and Guidelines to Combat Cybersecurity

The United States and European Union security agencies have updated their cybersecurity policies and mandates, specifying Zero Trust architectures, encryption, and post-quantum cryptography (PQC).

The European Union Network and Information Security (NIS2) directive established a unified framework to uphold cybersecurity across Europe. Additionally, the EU introduced the Digital Operations Resilience Act (DORA) that defines policies specifically tailored to the financial sector.

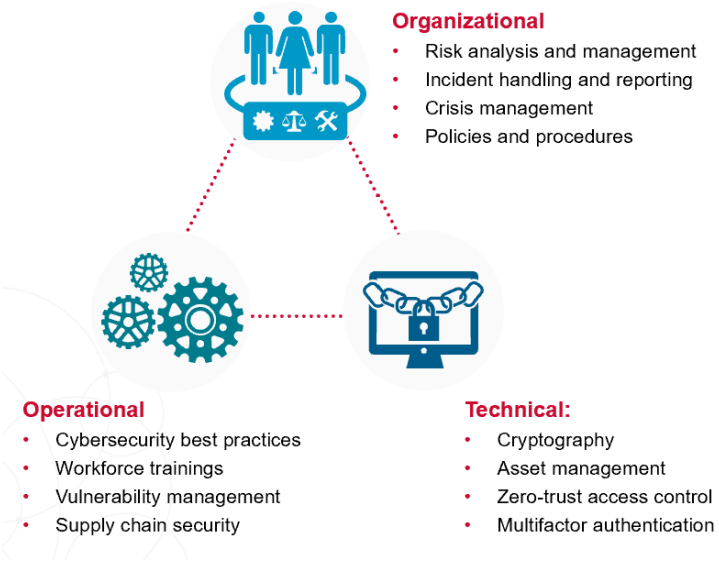
Due to their critical role in the economy and society, the following organizations are considered essential entities, and are therefore subject to stricter cybersecurity obligations: energy, transport, finance, health, drinking water, digital infrastructure, space, wastewater, and public administration. These entities must implement risk management measures, report incidents, and undergo regulatory oversight.

Figure 1: NIS2 Essential Entities

In comparison to U.S. Cybersecurity requirements such as CNSA, NIS2 and DORA focus less on technical requirements and more on mandating best practices, with a focus on ensuring organizations have proper procedures for preventing, as well as responding to, a cyber attack. There are also specific reporting mandates in the event of a breach.

This summary applies equally to NIS2 and DORA. It should be noted that while banking institutions are considered essential entities by NIS2, in practice they are held accountable to the DORA requirements.

Figure 2: Overview: DORA/NIS2 Cybersecurity Measures



NIS2 and DORA require organizations to implement Zero Trust mechanisms, which the server industry has been improving with each new generation of server. Secondly, it specifically requires organizations to evaluate cryptography and encryption "where appropriate", and to stay abreast of state of the art in this space.

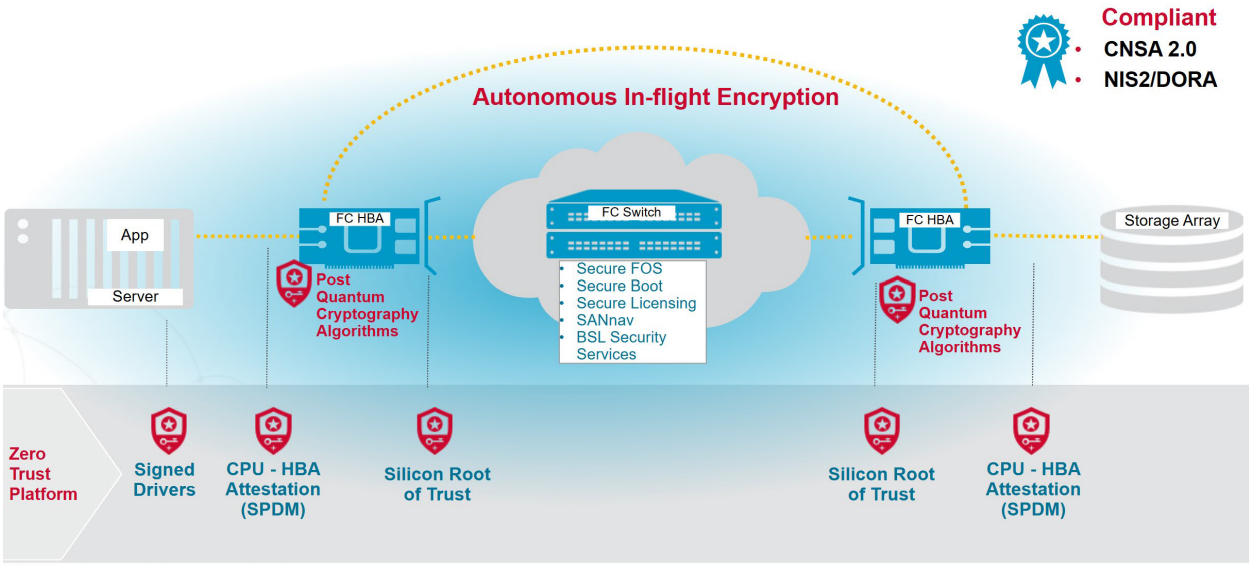
This paper examines the Emulex SecureHBA implementation of advanced security features that not only meet, but exceed compliance with the newest government data security mandates.

The Solution

Emulex solutions have taken critical steps to enhance the end-to-end trust data security throughout the data path, and to ensure Fibre Channel networks remain the most trusted architecture for the modern data center. The end-to-end security blueprint shown in Figure 3 highlights the critical role of the Fibre Channel host bus adapter (FC HBA) with a combination of several features to support a secure storage area network:

- Autonomous in-flight encryption
- Post-quantum cryptography
- Secure firmware
- HBA attestation to the host

Figure 3: Emulex SecureHBA Fibre Channel Solution: The Blueprint for a Zero Trust Data Center



PQC-Supported Features on Emulex SecureHBAs

Emulex SecureHBAs support the following PQC algorithms:

PQC-Enabled Feature	Implementation
Silicon Root of Trust (RoT)	LMS digital key signature (CNSA 2.0)
Security Protocol and Data Model (SPDM) Attestation	ML-DSA-87/ML-KEM-1024 digital key signature (CNSA 2.0)
Autonomous In-Flight Encryption (EDIF) INCITS FC-SP-3	AES-GCM-256 with ML-DSA-87/ML-KEM-1024 digital key signature (CNSA 2.0)

PQC-Enabled Silicon Root of Trust Firmware Security

Protecting the firmware on server motherboards with hardware-based security has become a generally accepted data center best practice. However, this motherboard security does not protect the firmware of intelligent peripherals like the FC HBA.

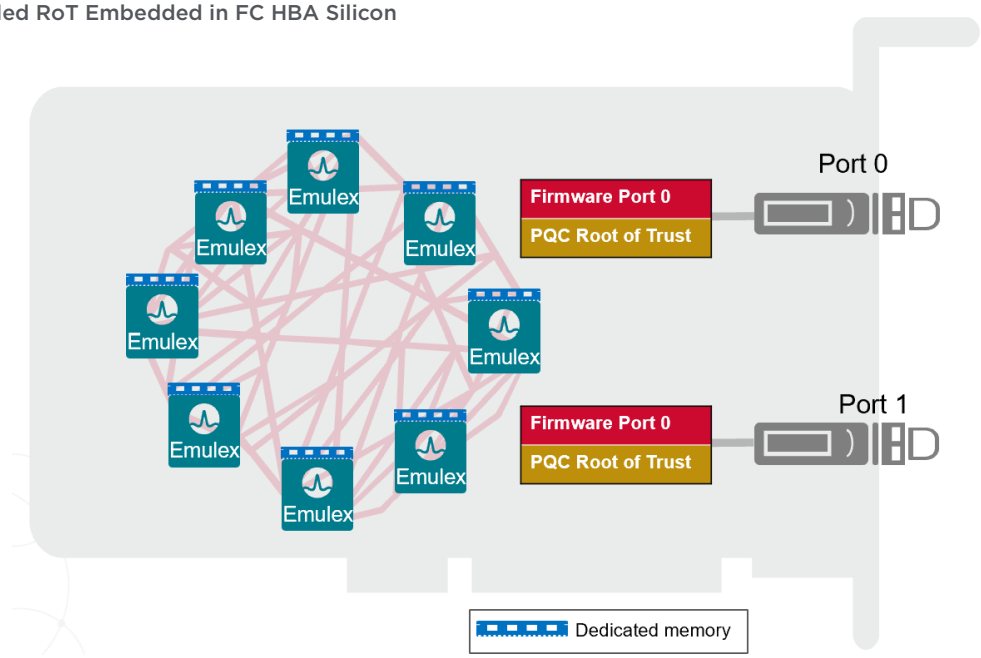
Adapter firmware must be secured by a lower-level protection mechanism, the silicon of the device itself. A true silicon root of trust (RoT) uses unalterable hardware to ensure the authenticity and integrity of all adapter firmware before it is allowed to execute on the controller. To make such an assurance, the RoT must guarantee the integrity of the controller boot process. The following is an explanation of the process.

How Does it Work?

1. Built-in trust: The RoT is embedded directly into the silicon of the FC HBA. The silicon has its own small, private, and secure key that cannot be changed or accessed by anyone other than the FC HBA itself.
2. Integrity of the firmware during boot: When the device powers on, the RoT is the first thing to activate. It confirms the firmware is tamper free.
3. Verify firmware upgrades: If the RoT detects the firmware has been updated, it starts a verification process and, only if the firmware is verified to be authentic, the FC HBA continues to boot up and work normally.

The Emulex SecureHBA is cryptographically signed with a PQC Leighton-Micali Signature (LMS) digital key signature. This is a significant advancement to the RoT feature, as the previous generation of HBAs do not support PQC algorithms.

Figure 4: PQC-Enabled RoT Embedded in FC HBA Silicon



The silicon RoT in Emulex FC HBAs provides strong, hardware-based security. The unalterable silicon RoT protects adapter initialization and operational firmware from compromise. Emulex FC HBAs create a PQC digital fingerprint in the hardware, ensuring the server never boots with compromised FC HBA firmware.

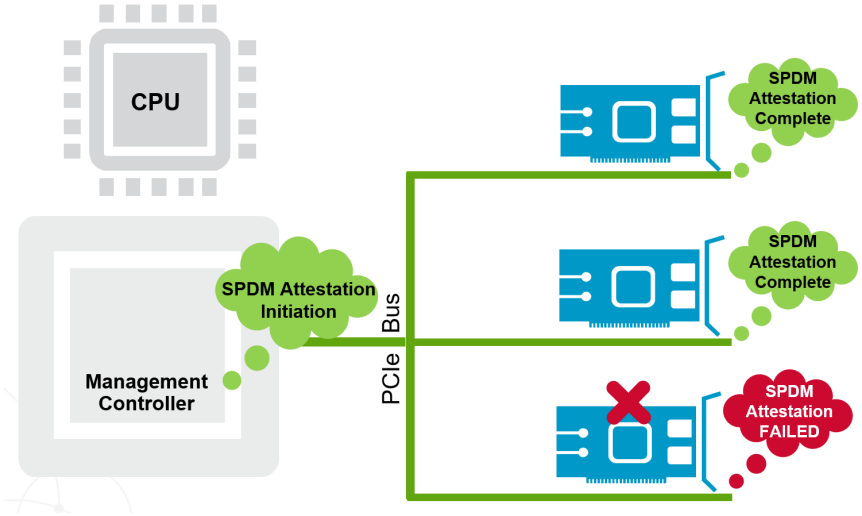
Security Protocol and Data Model Specification Attestation

The primary goal of the Emulex solution's implementation of the Security Protocol and Data Model (SPDM) Specification is to enable a server to cryptographically verify the identity of each Broadcom® adapter before it can send data across the PCIe bus. SPDM accomplishes this in the following manner:

1. Ensures secure communication: SPDM defines how devices should communicate with each other securely over the PCIe bus. It includes how they authenticate each other (prove their identities) and how they encrypt the information being exchanged to protect it from hackers.
2. Attestation: An SPDM-enabled FC HBA uses attestation to confirm its identity to the server management controller. SPDM ensures that both the device sending the data and the device receiving the data are verified.
3. Secure data exchange: The ultimate goal of SPDM is to make sure that devices can safely exchange data.

The Emulex SecureHBA SPDM feature provides identity assurance and data security communication with support for both ECDSA 384 digital key and PQC-enabled ML-DSA87/ML-KEM-1024.

Figure 5: The Host Management Controller Only Allows I/O Communication with SPDM-Authenticated Entities



PQC-Enabled Autonomous In-Flight Encryption

One method of data security is in-flight encryption; however, it has experineced limited enterprise adoption for several reasons:

- Significant performance overhead: Software and application-based solutions negatively affect server performance when encrypting and decrypting data.
- Key management is complex: Centralized and secure systems have complex and resource-intensive key creation, storage, expiration, and replacement processes that are disruptive and cause downtime.
- High cost: Software licensing costs, combined with the operational cost of management including compliance, monitoring, and access control, add significant cost.

This breakthrough in-flight encryption feature has been verified in third-party testing by StorageReview.com. The published report can be accessed at: docs.broadcom.com/doc/storagereview-emulex-secure-fc-hba. The highlights of the Emulex solution are as follows:

Session-Based Encryption

The Emulex SecureHBA is a simple, session-based encryption solution. Based on the emerging ANSI/INCITS FC-SP-3 standard, the session-based key management solution does not require complex and expensive key management software. Establishing an encryption session between a SecureHBA and a storage array port is quick, works with current SAN switches, and does not require any fabric management changes. Performed entirely in hardware, at port login, both endpoints will validate security capability, perform authentication and association, and begin encrypting Fibre Channel frames. Security session key refreshment happens automatically without traffic interruption.

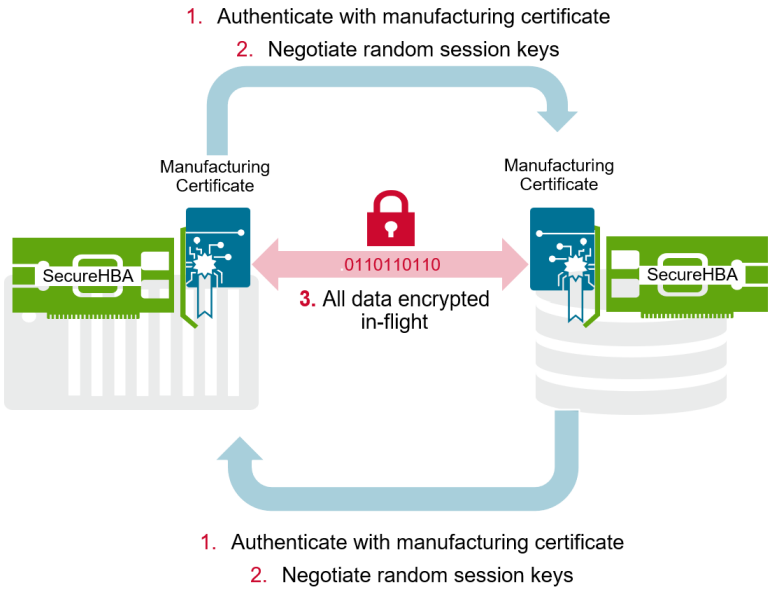
Hardware-Offload Encryption

Hardware-offload encryption architecture directs cryptographic tasks to a dedicated hardware engine inside the HBA. This offloading reduces the computational burden on CPUs while accelerating encryption processes. This approach is particularly effective in enabling broad usage within the data center without impacting overall performance. It allows organizations to achieve robust, scalable, and energy-efficient encryption without compromising performance.

PQC-Enabled, Simplified Key Management

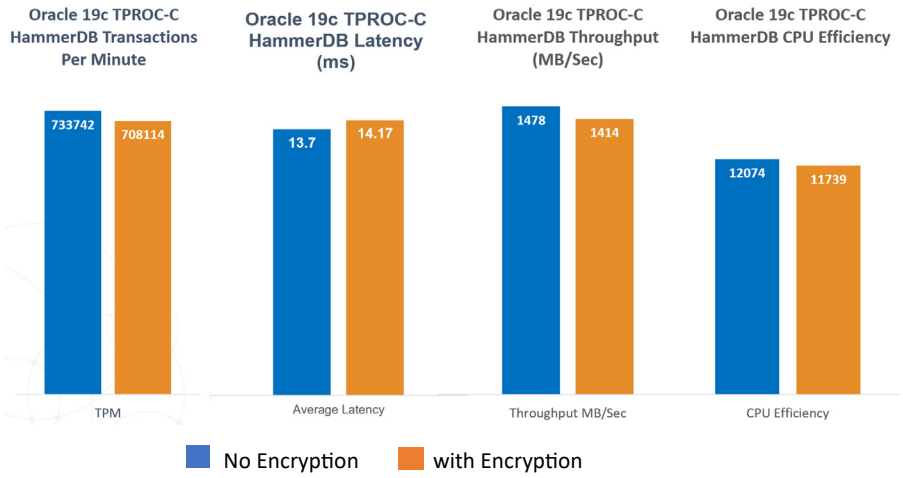
The SecureHBA implementation of session keys eliminates the complexity of an external key management server/software. The HBAs authenticate using the PQC-enabled ML-DSA-87, ML-KEM 1024 certificates. After authentication, random session keys are negotiated and generated by the HBAs deployed in the server and the storage array. Using the random session key, all data exchanged between the server and storage is encrypted using the AES-GCM-256 algorithm, as shown in Figure 6.

Figure 6: Autonomous In-Flight Encryption: Emulex SecureHBA Eliminates the Complexity of External Key Management Software Applications



Using real-world database application benchmarks, Emulex SecureHBA delivers wire-speed encryption without application performance degradation.

Figure 7: Emulex SecureHBA Autonomous In-Flight Encryption Performance: The Architecture Delivers Maximum Transaction, Latency, Throughput and Efficiency Performance via Hardware-Based Encryption of Data In-Flight (EDIF).



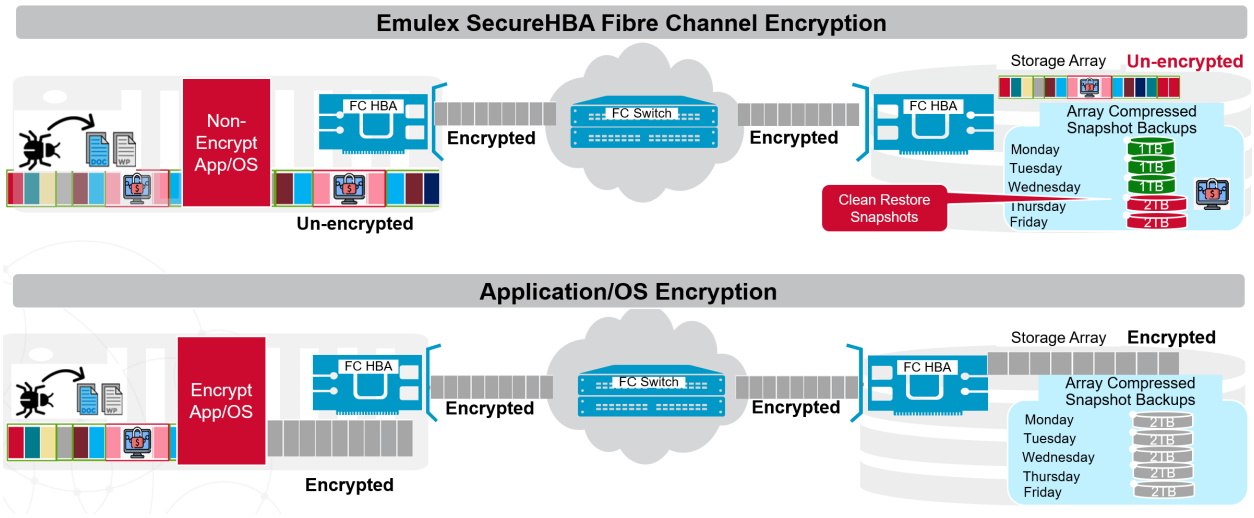
Ransomware Detection

Ransomware detection is critical to protect systems and data from malicious attacks. Best practices for detecting ransomware early can prevent or minimize damage from an attack. These three elements are ransomware detection best practices:

1. Protect: Protect data from becoming a target of cyber attacks and keep regular backups of important data.
2. Detect: Monitor and identify abnormal behaviors like file encryption and abrupt increases in the size of data, and trigger real-time alerts.
3. Recover: Using snapshots of previous backup copies of the data, revert back to the copy of the data prior to the cyber attack. Snapshots with historically consistent compression ratios are believed to be clean backups.

Since ransomware is encrypted, it alters the compression ratio of the snapshot backup. As shown in Figure 8, the data from the SecureHBA entering the storage array is decrypted, allowing the storage array to compress the data before storing on the SSD/HDD, so any abnormal increase in the size of the daily snapshot of the data can be detected. An increase in data size can signal a ransomware attack. Snapshots with historically consistent compression ratios are believed to be clean backups. In contrast, the data encrypted by an application/OS cannot be compressed and ransomware is harder to detect.

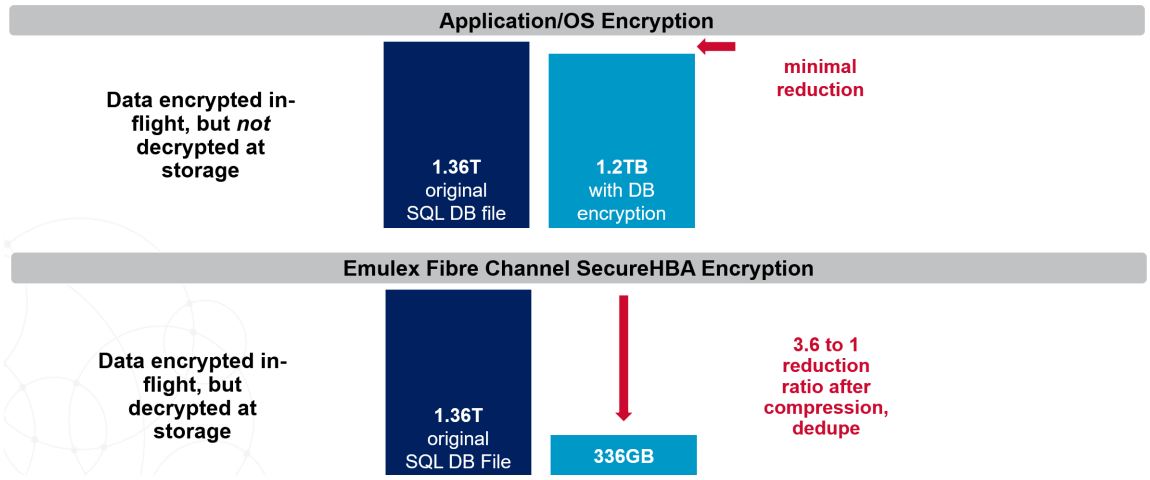
Figure 8: Array-Based Ransomware Detection. Application/OS-based Data Encryption Hides Ransomware-Infected Files. Emulex SecureHBA Encryption Enables Array Ransomware Detection Feature to Identify Infected Files.



Encrypt All Data and Preserve Storage Array Services

The Emulex SecureHBA encrypts all Fibre Channel data, unlike application-based encryption that only encrypt the data associated with the particular application. Furthermore, since all data is decrypted once it reaches the storage array, all the critical value-add services of a storage array are kept intact, such as data compression and data deduplication to manage the storage array capacity. Figure 9 shows the storage array ability to substantially reduce the storage utilization with the Emulex SecureHBA, as opposed to an application-based encryption solution.

Figure 9: Application-Based Encryption Restricts the Ability to Compress, Deduplicate. The Emulex SecureHBA Preserves the Data Capacity Reduction Services of the Storage Array.



Summary

As enterprise security threats grow in scale and sophistication, protecting data in motion has become as critical as securing data at rest. Enterprise customers must also be aware of the clear and present danger of harvest now and decrypt later threat models utilizing upcoming quantum computers, which has driven government security experts to set new post-quantum cryptography standards. Traditional software encryption solutions introduce performance trade-offs that many organizations simply can't afford, as well as rendering some storage array services as useless. The Emulex SecureHBA changes that equation by delivering PQC-enabled, standards-based, hardware-offloaded encryption that seamlessly integrates into existing servers and Fibre Channel SANs while enhancing the adapter attestation and firmware security to meet the PQC standards. To summarize, Emulex SecureHBAs provide a range of benefits:

- Solve issues with existing in-flight encryption solutions by delivering maximum performance and session-based key management; built upon an affordable standards-based platform.
- Enable enterprises to comply with government regulations such as CNSA 2.0, NIS2, DORA, and more with Zero Trust architecture, and encryption with PQC algorithms.
- Preserve storage array services such as ransomware detection, compression/deduplication.
- Easy to deploy in existing Fibre Channel infrastructures.

BROADCOM®
connecting everything®

For more product information: broadcom.com

Copyright © 2025 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
SecureHBA-Encryption-EMEA-SB100 May 28, 2025