TEST REPORT

Tolly.

#225146

September 2025

Commissioned by Broadcom

Broadcom Emulex LPe38102 64G SecureHBA

Security Features & Performance vs. Marvell QLogic QLE2872

EXECUTIVE SUMMARY

Security is no longer a convenience it is a requirement. New regulations have gone into effect worldwide in 2025 that mandate new best practices for zero trust and security with implementation beginning this year. The security threats are real. Financial losses due to data breaches, cyber-attacks and un-authorized access are an increasing pain point for businesses. New-generation Intel Granite Rapids servers are now shipping from all major OEMs with full 64GFC support, delivering major improvements to datacenter performance and security.

Broadcom commissioned Tolly to validate the security features and performance of the Broadcom Emulex 64G LPe38102 SecureHBA compared to the Marvell QLogic QLE2872 HBA.

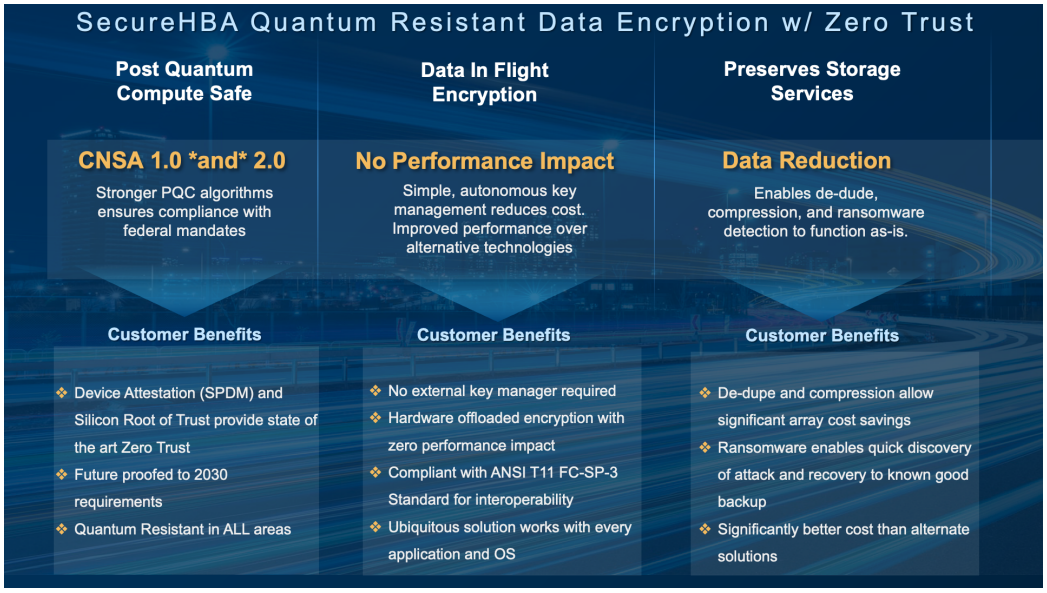
Tests showed that the Broadcom Emulex HBA provides a suite of high-security features including device attestation - SPDM (Security Protocol and Data Model), Silicon Root of Trust (Si-RoT), secure boot, digitally signed drivers, and other features that exceed current security requirements and are not available in the QLogic HBA. The Emulex SecureHBA, with encryption enabled, demonstrated better performance than QLogic, without encryption, in the microbenchmarks and Oracle database transaction tests. See Figure 1 & Table 1 for a summary of results.

THE BOTTOM LINE

The Emulex LPe38102 SecureHBA adapters vs. the competition delivered:

1. Superior security features with full 64G FC performance, and with better performance running encryption than competitive HBA *without* encryption
2. Better Oracle Database performance with 51% greater transactions per minute, 67% better CPU efficiency, and 46% lower latency
3. Up to 187% better small block size 64G FC link utilization, which was significantly better than the competitive HBA that delivered 32% of the FC maximum for 4K blocks, and 58% for 8K blocks

Broadcom Emulex SecureHBA
Leading-Edge Security Features



Source: Tolly, May 2025

Figure 1

Test Results

Security

Security is important at every level. New government regulations are meant to protect industries from these threats by requiring improvements in security implementations. In the European Union (EU), NIS2[1]/DORA are in effect today. Companies must comply. Mandates include a stronger level of zero-trust, multi-factor authentication (MFA) best practices, and it requires that an organization form a policy on the use of encryption/cryptography.

In the US, companies are encouraged to implement CNSA 1.0 in 2025 and there is a mandate to move toward more stringent CNSA 2.0 by 2030. CNSA 2.0 specifies the use of zero trust (SPDM, zero-trust device attestation) and specifies specific algorithms for PQC. It mandates the use of encryption both at rest and in flight. See Figure 2.

Government Requirements

Figure 2

The Emulex SecureHBA supports both versions 1.0 and 2.0 of the US National Security Agency's (NSA) Commercial National Security Algorithm (CNSA) suites. CNSA 2.0 is notable for its inclusion of Post Quantum Cryptography (PQC) algorithms. The QLogic HBA supports Si-Rot under CNSA 1.0. See Table 1.

The Emulex SecureHBA introduces autonomous in-flight encryption which is a based on the INCITS Fibre Channel FC-SP-3 industry standard. The Emulex SecureHBA offers hardware-accelerated encryption of data in flight (EDIF), incorporating post-quantum cryptography (PQC) and Zero Trust

Comparative Security & Performance Summary

	Emulex SecureHBA		QLogic QLE2872	
Security Level	CNSA 1.0	CNSA 2.0	CNSA 1.0	CNSA 2.0
Autonomous In-flight Data Encryption	Yes. Session-based keys		No. Requires key management software	
Si-RoT	Yes	Yes	No (Yes for Dell-Branded QLE2872C)	No
SPDM	Yes	Yes	No	No
	Performance			
IOPS (Manufacturer product specification)	Up to 10M IOPS (64G)		2M IOPS (64G)	
64G FC Link Utilization	Designed to drive full 64GFC for high transaction apps		Only 32% of 64GFC link utilization at 4K data block sizes	
OLTP Database Performance	Up to 51% greater Database TPM than QLogic			

Source: Tolly, May 2025

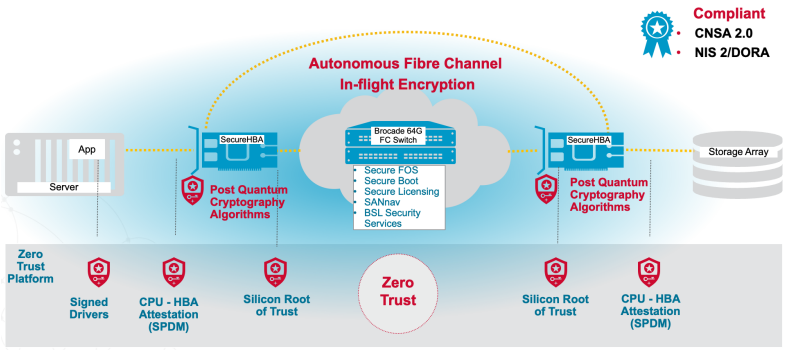
Table 1

[1] https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2

principles. With session-based key management, encryption keys are managed automatically by the HBA. When the HBA is communicating with another compatible HBA, the encryption is automatic and autonomous without need for configuration, manual session establishment, or external key management. Encryption does require a compatible array as shown in Figure 3 which provides an overview of all of the Emulex SecureHBA security features.

Storage array support is in development and arrays are forthcoming. When connecting to storage arrays that do not yet support autonomous in-flight encryption a connection will be established without encryption, as expected. The feature also does not require specific switch support. Importantly, the encryption does not degrade performance. For a visual depiction of the security features of the Emulex LPe38102 SecureHBA, see Figure 3.

Emulex Fibre Channel SecureHBA 64G Solution



Source: Tolly, May 2025 Figure 3

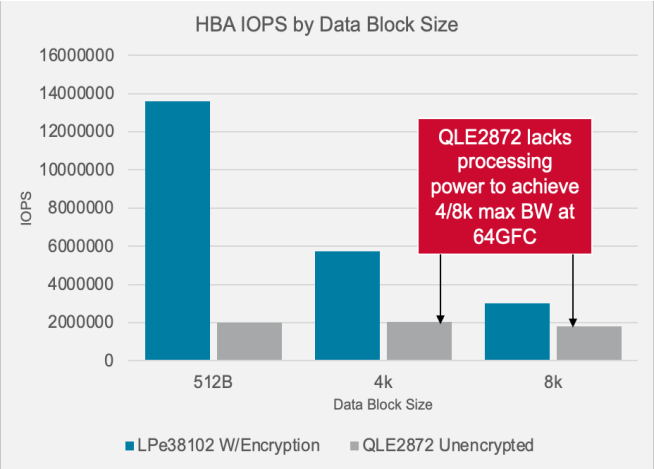
64G Performance

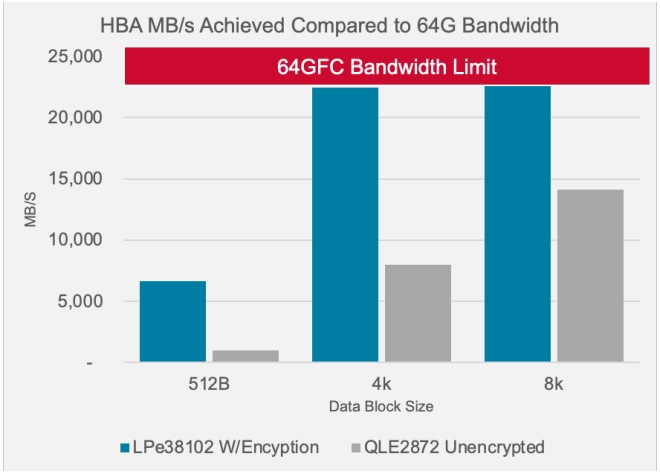
While secure communication is mandatory, it is essential that increased security does not have a negative impact on system performance.

Encrypting at the application level - within the server - not only increases costs due to software licensing but also due to the extra CPU cycles required of the server which will require higher performance and more expensive hardware to process the encryption.

Emulex implements its EDIF in hardware, thus avoiding the processing overhead of software encryption. Encryption, by design, adds some small overhead to each data packet traversing the FC link. Testing, discussed below, shows that the encryption overhead of the Emulex SecureHBA is negligible and, in fact, still outperforms the competitor (without encryption capability) in terms of 64G performance. See Tables 2-6 for detailed configuration information. The composite test bed is found in Figure 7.

FIO Performance 2x64G FC Read/Write
(as reported by FIO)





Source: Tolly, May 2025 Figures 4a & b

FIO Microbenchmark

FIO (Flexible I/O Tester) is an open-source tool used for benchmarking storage performance by generating various I/O workloads, such as random or sequential reads and writes. It allows users to measure metrics like IOPS (Input/Output Operations Per Second) and throughput, making it suitable for testing different storage systems.

This benchmark stresses the storage system - and the FC links in between server and storage targets, at a very low level and is used to drive these systems to maximum levels.

These tests used both ports of each HBA and measured the IOPS performance and resultant full-duplex throughput of the two HBAs in comparison to each other, and to the calculated link maximum for 64G Fibre Channel. In general, processing smaller data block sizes requires more processing power from an HBA's processors, making the IOPS specification of the product a good indicator of its ability to run workloads at 64G FC.

4K and 8K block sizes reflect the data size most used by high transaction applications such as databases. Here the Emulex SecureHBA is powerful enough to drive IOPs at over 92.4% of 64G FC link maximum, reinforcing the importance of its 10M IOPS product specification to get full value from 64G Fibre Channel. Results show that the HBA exceeds the product performance specification of 10M IOPS at 2K block size. See Figures 4a, 4b, & 5.

By contrast, the QLogic HBA trailed in all scenarios. Figure 4a shows the IOPS hit the ceiling of 2,000,000 IOPS. Figure 4b translates that into data throughput which is far below both Emulex and the maximum bandwidth for 64G FC. Figure 5 adds two additional frame sizes, 2K and 64K, and interprets the results as a percentage of link maximum. For the important database sizes of 4K and 8K, QLogic's maximum IOPS represent 32% and 58% of theoretical maximum respectively.

HammerDB Oracle Database Benchmark

HammerDB is an open-source database benchmarking application designed to simulate a load of actual users accessing a database. In this test, the database was located on an FC target. The TPROC-C profile ran twice, with encryption enabled and then disabled for the Emulex SecureHBA.

Broadcom

Emulex LPe38102 64G SecureHBA

Security Features & Performance

Tolly. Certified

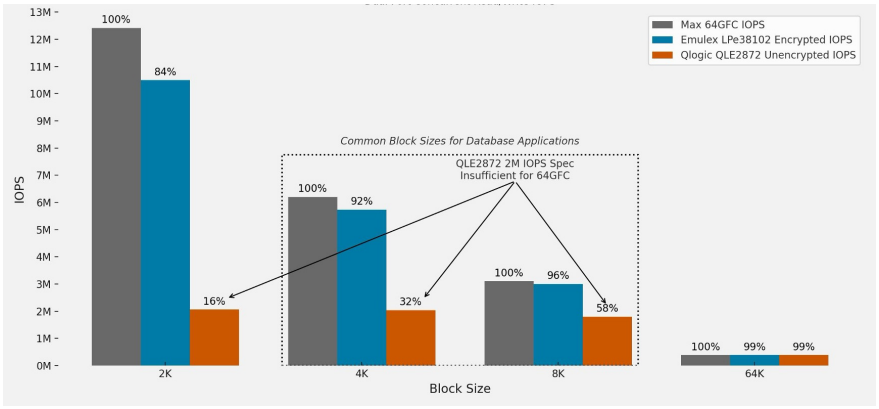
Tested May 2025

Results were analyzed as transactions per minute (TPM), server CPU efficiency, and stored procedure latency.

Because this test simulates 256 users accessing the database, results of consecutive runs with identical settings will vary somewhat. The results of these two test runs are virtually identical illustrating that there is negligible impact running EDIF enabled. See Figure 6 (next page).

The same tests were run again using the QLogic HBA in the server. When compared, the Emulex SecureHBA TPM

Emulex SecureHBA - Encryption Enabled
Dual-Link IOPS vs. 64GFC Link Maximum
(as reported by FIO)

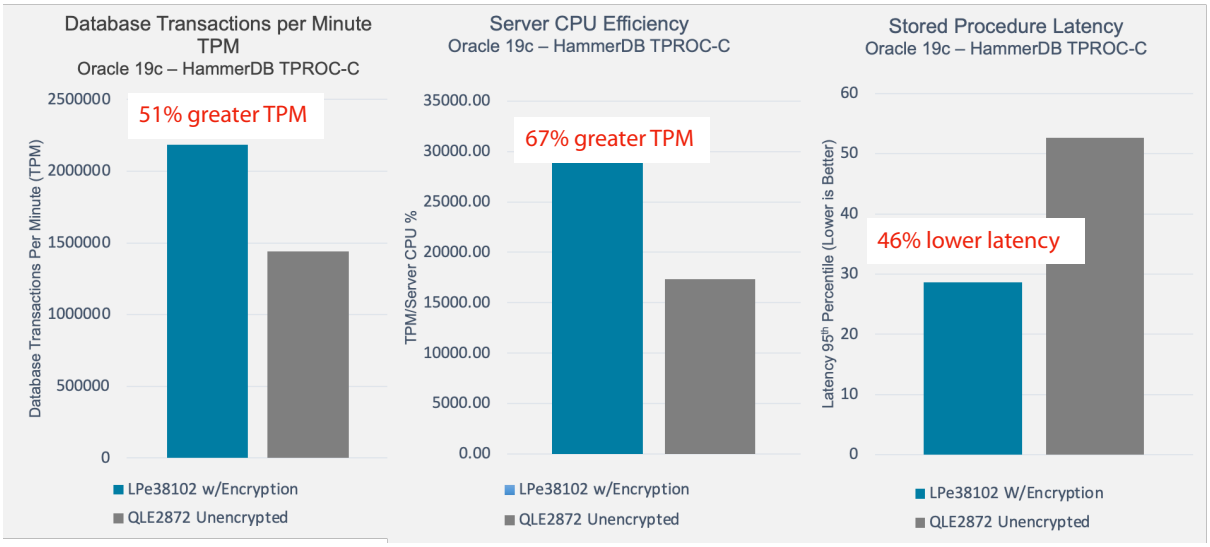


Source: Tolly, May 2025

Figure 5

results were 51% greater than QLogic. Similarly, the CPU efficiency (TPM/ server CPU) was 67% better for the Emulex SecureHBA. Finally, the 95th percentile stored procedure latency was 46% lower (better) than QLogic.

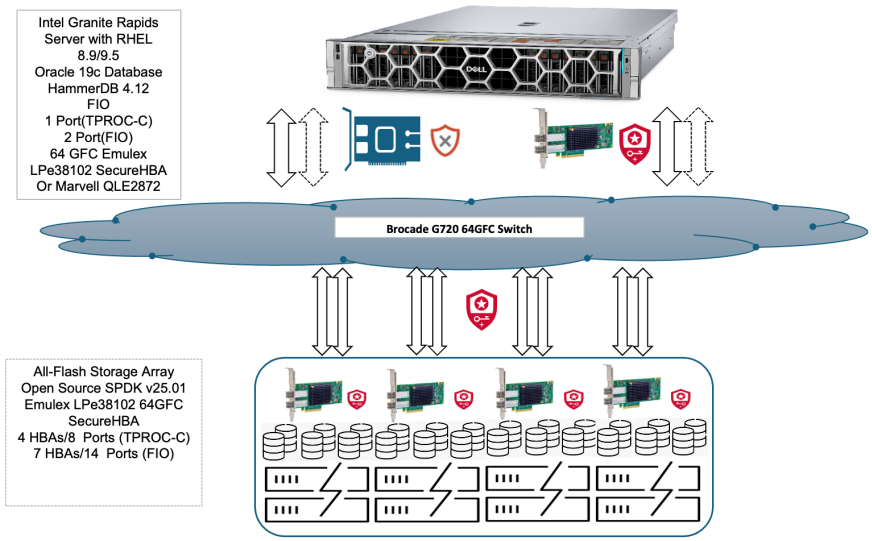
Emulex SecureHBA - Encrypted vs. Non-Encrypted
Oracle 19c Database Performance
(as reported by HammerDB)



Note: Blue bars represent encrypted performance, gray bars represent unencrypted performance.
Source: Tolly, May 2025

Figure 6

Composite Test Bed Topology



Source: Tolly, May 2025

Figure 7

Test Configuration Summary

64G HBAs Under Test

Vendor	Product Name	Firmware	LPFC Driver	Settings
Broadcom	Emulex LPe38102 64G SecureHBA FC	14.14.436.7	14.4.393.31	Autonomous in-flight data encryption enabled; 7-day key exchange; Post-Quantum Cryptography (PQC) - CNSA 2.0
Marvell	QLogic QLE2872	9.15.03	10.02.12.01-k	

Table 2

Server Configuration

Vendor/System	Intel Granite Rapids
CPU	2x Intel(R) Xeon 6 (R) 6767P @ 2.4GHz
Number of CPUs	128 processors. Profile: Performance
Memory (RAM)	256 GB
Versions	BIOS 1.2.6; FW 1.20.25.00
OS	Red Hat Ent. Linux 8.9 (RHEL8)
Kernel Settings	Numa = off; Transparent huge pages = disabled; Huge Pages size - 2MB

Table 3

Storage Configuration

Vendor/Device	Non-branded all-flash storage array
Software	Based on open-source SPDK target v25.01
HBAs	8 to 14 x 64G FC target ports of Emulex SecureHBA
Settings	See Table 2, Broadcom HBA
Network Fabric	Brocade G720 64GFC Switch v9.1.1

Table 4

Database Test Tool

Application	Open Source HammerDB 4.12
TPROC-H settings	Total Number of Warehouses: 2000; Transactions per User: 1 million; Number of Virtual Users: 256; Ramp-up. Time: 1 minute; Run Time: 3 minutes.
Metrics Used	TPROC-C: TPM is the number of user commits plus the number of user rollbacks. TPROC-C : NOPM (New Orders per minute) is a metric captured from within the test schema itself and is the recommended primary metric to use. TPROC-C : Time profile for all the stored procedures for TPROC-C workload Linux SAR CPU Utilization and DSTAT IO Throughput

Table 5

Oracle Database Configuration

Database	Oracle Database 19c (19.3)
Storage Type	Oracle Grid 19c; ASM Disk group external redundancy (DATA: 16 disks; LOGS/OCR: 8 disks); oracleasmlib-2.0.17-1
Database Settings	TEMP Tablespace: 30GB Big data file; TPROC-C Tablespace: ~160-200GB Big datafile; UNDO Tablespace: 70GB; ONLINE REDO LOGS: 8 x 6GB each; Block Size: 4-16KB; SGA: 32G, PGA 12G

Source: Tolly, May 2025

Table 6

About Tolly

The Tolly Group companies have been delivering world-class IT services for over 35 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at: http://www.tolly.com

Emulex LPe38102 64G SecureHBA FC

The Broadcom Emulex SecureHBA adapters are secure, high-performance, 32/64G FC HBAs providing post-quantum security protection.

- Emulex SecureHBAs introduce autonomous data In-flight encryption with session-based key management (per FC-SP-3 INCITS 577-202x). Encryption keys are managed automatically by the HBA, with support for Post Quantum Cryptography (PQC) via CNSA 2.0 compliant algorithms, as well as CNSA 1.0.
- Device attestation – SPDM (Security Protocol and Data Model) utilizing IPS 203 and 204 compliant algorithms ensures that only authentic devices can communicate on the PCIe bus. PQC compliant CNSA 2.0 and CNSA 1.0 supported.
- Silicon Root of Trust (Si-ROT) (NIST SP 800-193 compliant) hardened with both PQC compliant CNSA 2.0 and CNSA 1.0 algorithms – only authentic firmware can be loaded.
- Additionally, Emulex's Zero Trust Architecture includes Secure Boot, Digitally signed Drivers, plus T10-DIF for data integrity

Terms of Usage

225146 czse-14a -wt 2025-09-16 VerM