StorageReview

January 2025

Emulex Secure HBAs: The New Standard for In-Flight Network Encryption

Intro

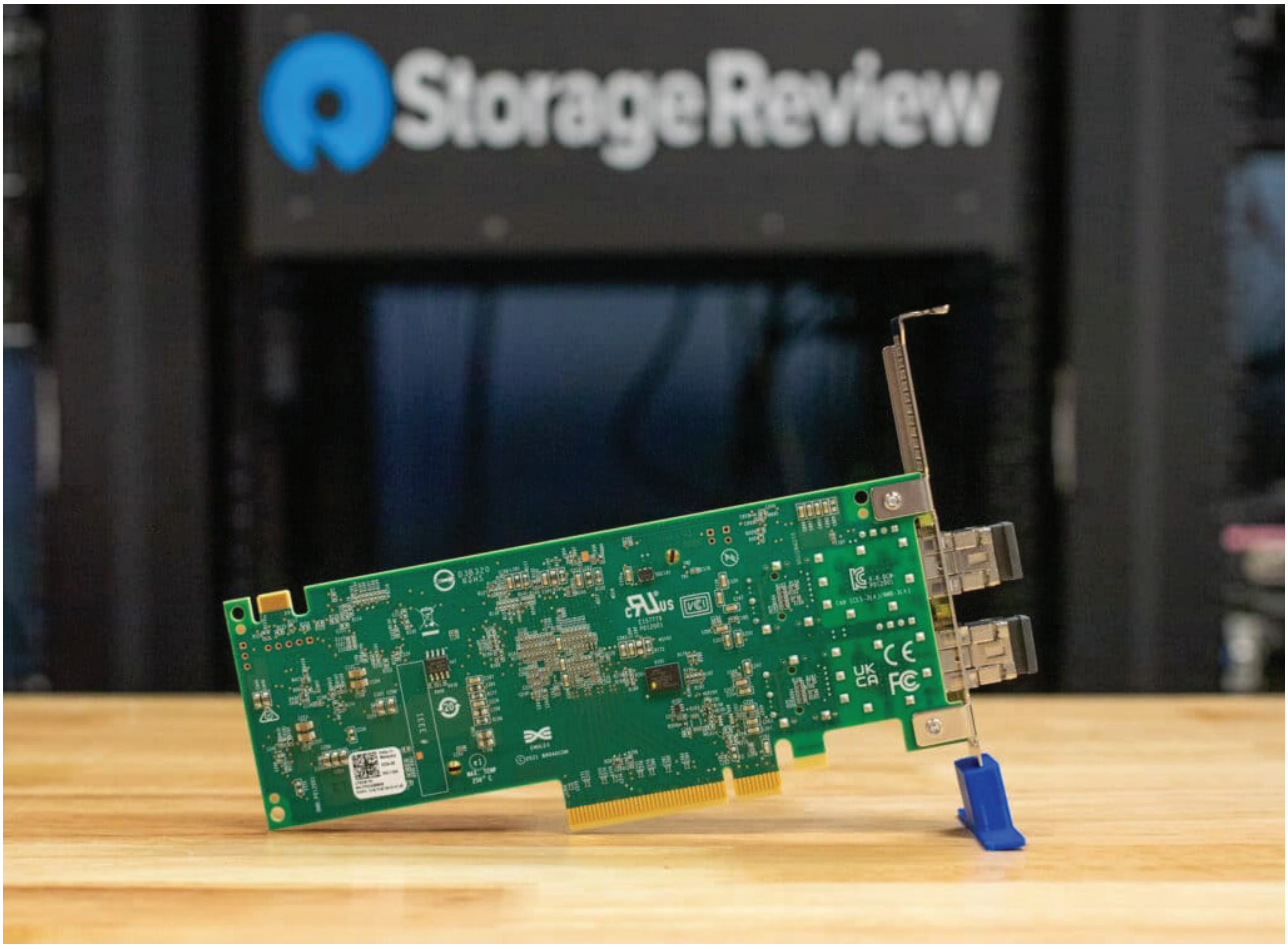
The growing sophistication and frequency of cyberattacks on enterprise data centers demand robust and comprehensive security measures. Traditional firewall-based approaches are increasingly inadequate to protect sensitive information, particularly as attackers exploit vulnerabilities in internal data flows. Ensuring data security in transit has become a critical focus, and in-flight encryption offers a powerful solution to prevent data breaches and unauthorized access within storage area networks (SANs).

Enter the Emulex Secure Fibre Channel Host Bus Adapters (HBAs), a data center security breakthrough. These HBAs deliver robust, session-based encryption for Fibre Channel SANs, enabling enterprises to adopt a zero-trust approach to internal data traffic. With compliance to stringent standards like the forthcoming Fibre Channel Security Protocol (FC-SP-3) and Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), Emulex Secure HBAs provide quantum-resistant encryption that operates seamlessly within existing infrastructures. Notably, these solutions are hardware-offloaded, ensuring that security enhancements do not compromise performance.

Customers have been reluctant to deploy in-flight encryption solutions (EDIF) for several reasons, including high cost, complexity, and significant application performance degradation. The StorageReview Lab team has experienced and documented the same results when comparing software versus hardware encryption. The Emulex Secure HBA is ready to dispel those theories and put in-flight encryption at the top of the list for encrypting data in flight without crushing server performance while maintaining uncompromised throughput.

Another significant advantage of Emulex Secure HBAs is their seamless integration, particularly for storage array vendors. With encryption fully offloaded to the HBA hardware, storage vendors can maintain their focus on performance and array-specific functionalities without the burden of extensive software reengineering.

This ease of adoption is expected to drive widespread acceptance across the industry. The Fibre Channel industry's latest update of the security technical specification for Fibre Channel products, INCITS Fibre Channel Security Protocol 3 (FC-SP-3), establishes a standard for interoperable Fibre Channel products. This latest update includes the definition of protocols to authenticate Fibre Channel entities, protocols to set up session keys, and protocols to negotiate the parameters required to ensure frame-by-frame integrity and confidentiality.



Emulex engineers have been actively involved in standards development to ensure that Fibre Channel remains at the forefront of addressing security challenges required of the modern data center. As regulatory pressures mount and cyber threats evolve, adopting Emulex Secure HBAs ensures that SAN vendors can provide robust, future-proof security solutions with minimal effort. For enterprises using Fibre Channel, the current FC-SP-3 standard is crucial for future-proofing data security.

Through a hands-on demonstration, we will illustrate the benefits of deploying Emulex Secure HBAs, showcasing their ability to maintain high performance while delivering uncompromising security. From preventing data leakage to enabling real-time anomaly detection, these HBAs represent a significant leap forward in securing the enterprise data center against modern threats.

Understanding Emulex Secure HBA Technology

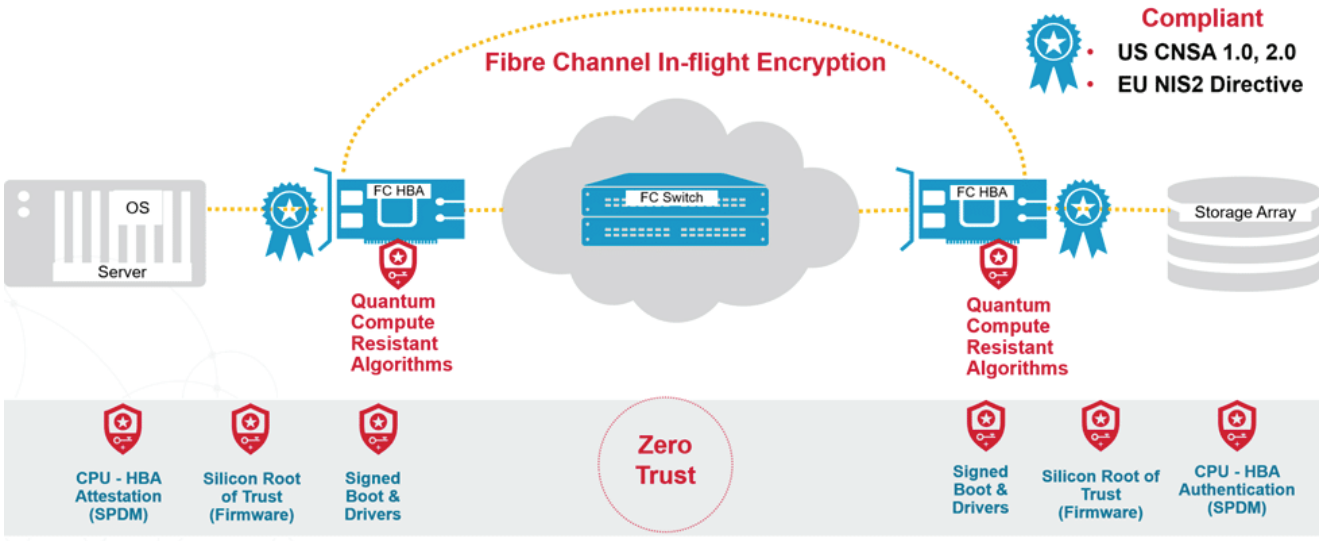
Overview of session-based encryption and zero-trust principles.

Session-based Encryption

The Emulex Secure HBA 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 prohibitively expensive key management software. Establishing an encryption session between a Secure HBA and storage array port is simple, 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, begin authentication and association, and begin encrypting Fibre Channel frames. Security session key refreshment happens automatically without traffic interruption. Since this is all done in hardware, software changes are not needed, and multipath software is unaffected. The solution supports backward compatibility by auto-negotiating with older arrays that may not be EDIF capable.

Zero-Trust

Zero-Trust security operates on the principle of "never trust, always verify," ensuring every access request is authenticated, authorized, and continuously monitored. Unlike traditional perimeter-based models, zero-trust minimizes the risk of breaches by requiring identity verification and enforcing least privilege access for users and devices.



Implementing zero-trust security has several core advantages. The continuous verification implemented with zero-trust reduces the overall attack surface. It is also adaptable, supporting hybrid workforces, cloud adoption, and seamless IoT integration. Of course, regulatory compliance is at the top of most countries' minds. Zero-trust aligns with stringent data security standards to meet evolving regulations.

Zero-trust ensures a resilient and adaptable security posture critical for protecting sensitive organizational data by leveraging multi-factor authentication, micro-segmentation, and behavioral analytics.

The Secure HBA introduces a quantum-resistant silicon root of trust to protect the integrity of the firmware and ASIC.

Hardware-offloaded Encryption

Hardware-offloaded encryption enhances performance and security by delegating cryptographic tasks to dedicated hardware gates inside the HBA. This offloading reduces the computational burden on CPUs while accelerating encryption processes.

Hardware-offloaded encryption delivers increased performance. Dedicated hardware accelerates cryptographic operations and reduces latency and processing. CPU cycles are freed up for other tasks, boosting overall system efficiency. Deploying isolated hardware modules makes it tamper-resistant and reduces vulnerabilities.

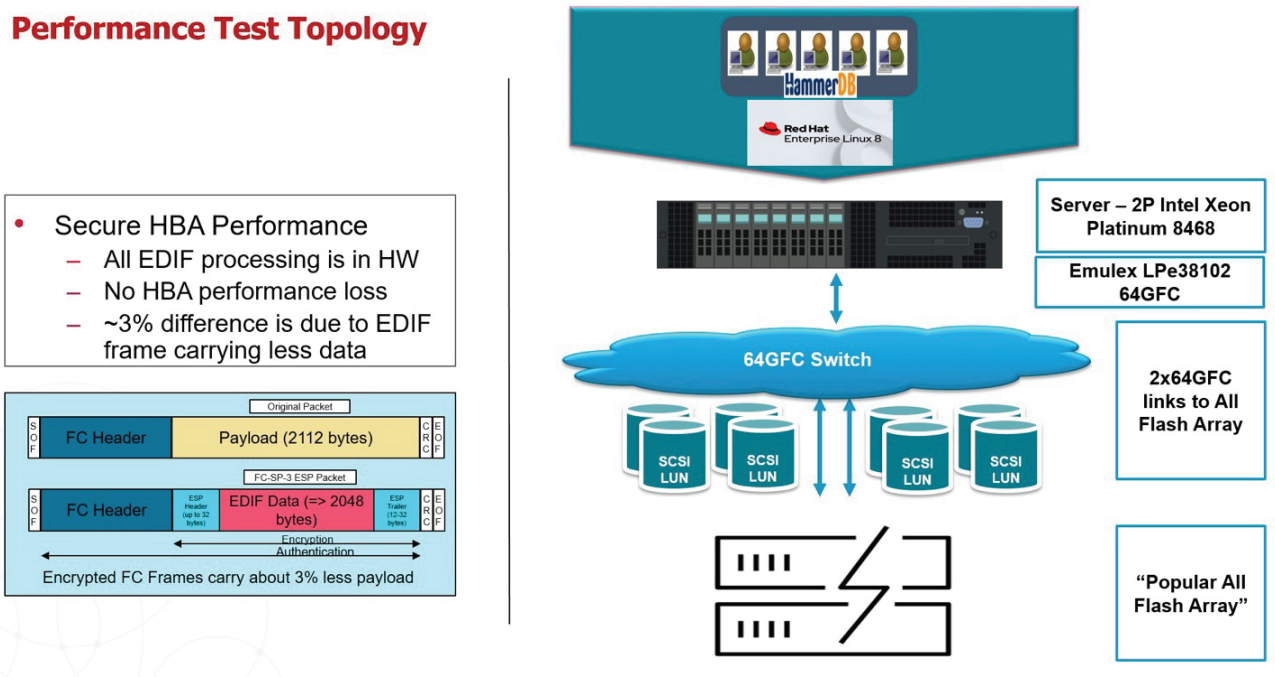
This approach is particularly effective in enabling broad usage within the data center without impacting overall performance. It allows organizations to achieve robust, scalable, and energy-efficient encryption without compromising performance.

Demonstrating the Benefits

Industry-standard plug-and-play encryption

Emulex ran us through a demo to showcase the minimal performance differences with encryption enabled and disabled to see how much overhead this solution adds to data in flight. The steps below describe enabling or disabling encryption on the Emulex Secure FC Host HBAs. The HBAs used in the host and array were the Emulex LPe38102 64G, which Emulex told us were made functional within the flash array with a simple driver update for test purposes.

Demo Topology



Emulex HBAs process all encrypted data in-flight (EDIF) in hardware. The HBAs have 8-core SoCs, which manage the workload and direct the data packets through the encryption offload engine. Since the encryption is offloaded, the host CPU is unaffected by those encryption operations.

The first exercise was to run a TPROC-H workload leveraging HammerDB as a database loadgen with EDIF disabled. The Emulex Secure HBA's default behavior is to enable EDIF when connecting to compatible target ports but also allow for backward compatibility if a target does not support EDIF. The Emulex hbacmd utility is used to turn off the EDIF function of the HBA port and verify the setting change.

```
[root@dhcp-10-231-153-170 ~]# cd HammerDB-4.12/
[root@dhcp-10-231-153-170 HammerDB-4.12]# hbacmd GetEDIFParams 10:00:70:b7:e4:22:ae:57

EDIF Params for 10:00:70:b7:e4:22:ae:57

EDIF-State                : Disabled
REN (Requires-Encryption) : Disabled
Rekey-Interval            : 7 (In days)

[root@dhcp-10-231-153-170 HammerDB-4.12]#
```

Once the setting was verified, we started the workload on the database. The read-heavy demo shows how much of the 64G FC pipe is used, which easily reached the line rate for the majority of the test.

Now, it's time to change the parameter to enable encryption on the HBA. Again, the Emulex hbacmd utility is used to turn on the EDIF function of the HBA port and to verify the setting change. The screen below shows the command and output. Simply setting the EDIF state to 1 turns on encryption in-flight. Set EDIF Parameter edif-state=1. The message "New edif parameter setting has been set" will be displayed if the change is accepted. It will be necessary to restart the host to make the changes to the EDIF state take effect.

```
Vuser 1:Geometric mean of query times returning rows (22) is 9.31075
^C
[root@dhcp-10-231-153-170 disable]# hbacmd SetEDIFParam 10:00:70:b7:e4:22:ae:57 EDIF-State 1

Set EDIF Parameter edif-state=1 for 10:00:70:b7:e4:22:ae:57


New edif parameter setting has been set.

[root@dhcp-10-231-153-170 disable]# hbacmd GetConnectionInfo 10:00:70:b7:e4:22:ae:57

                                                Post-Quantum      Days Until
   S_ID       D_ID          Peer WWPN           Cryptography        Rekey
---------- ---------- ----------------------  ----------------   -----------
0x10800    0x12000    52:4a:93:78:3c:20:00:0a       Yes               7
0x10800    0x12200    52:4a:93:78:3c:20:00:1a       Yes               7

[root@dhcp-10-231-153-170 disable]#
```

To verify that the change took effect, run the "hbacmd GetEDIFParams" command. The result indicates that the EDIF state is enabled, and the Required-Encryption option is disabled.

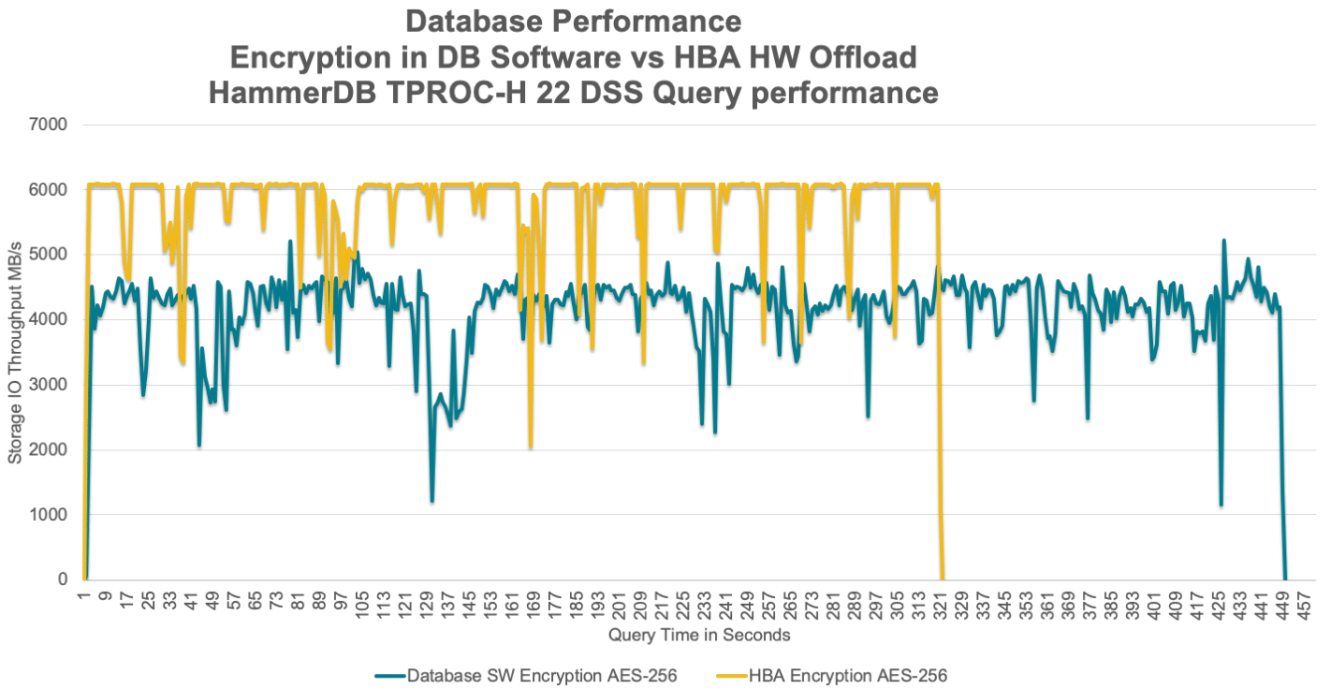
```
[root@dhcp-10-231-153-170 ~]# hbacmd GetEDIFParams 10:00:70:b7:e4:22:ae:57

EDIF Params for 10:00:70:b7:e4:22:ae:57

EDIF-State                : Enabled (default)
REN (Requires-Encryption) : Disabled
Rekey-Interval            : 7 (In days)
```

To verify the ports on the HBA are connected and EDIF is enabled, run the "hbacmd GetConnectionInfo" command. The output should look like the image below.

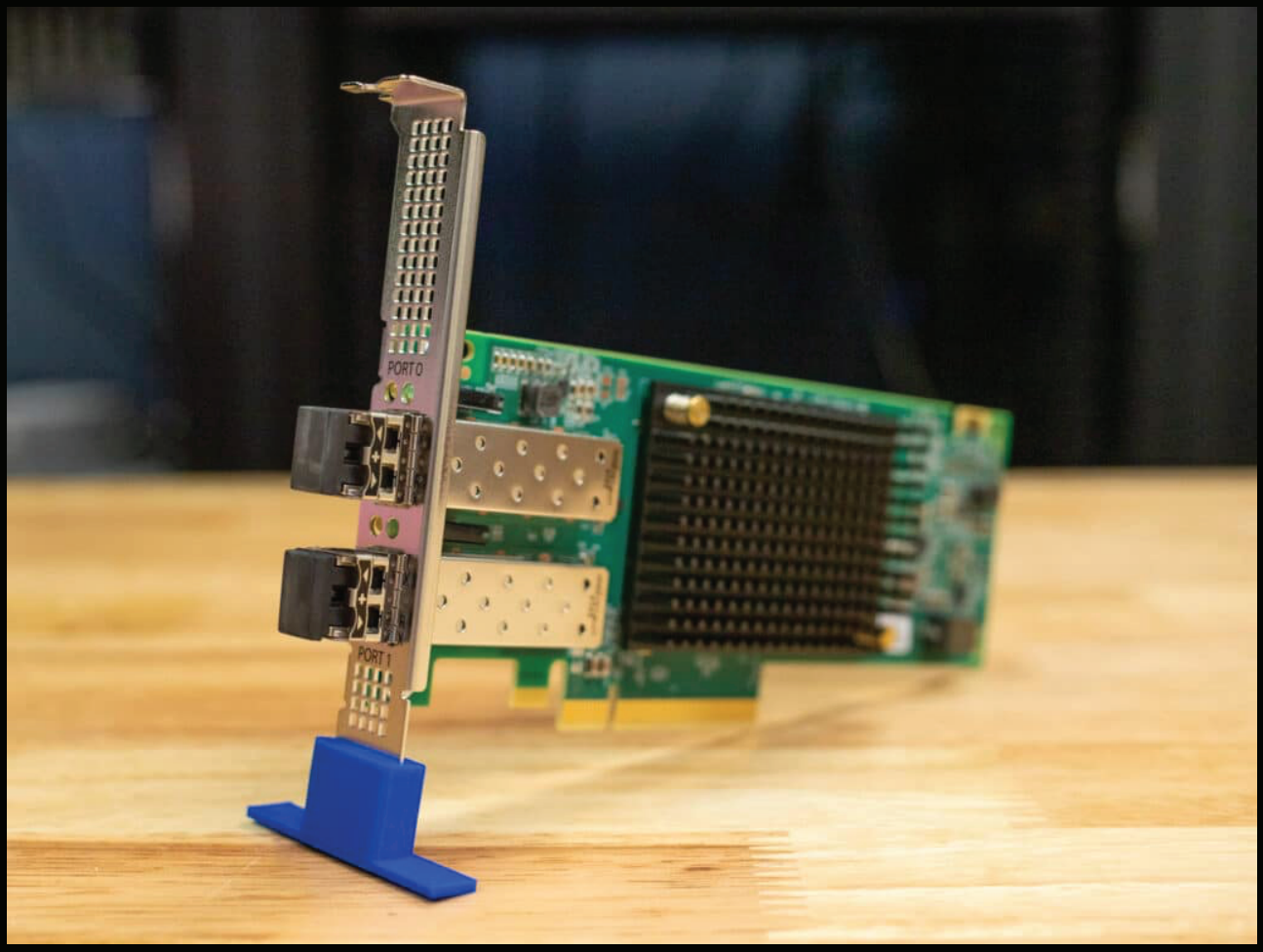
```
[root@dhcp-10-231-153-170 ~]# hbacmd GetConnectionInfo 10:00:70:b7:e4:22:ae:57

                                                  Post-Quantum      Days Until
   S_ID       D_ID          Peer WWPN             Cryptography       Rekey
---------- ---------- ------------------------  ----------------   -----------
0x10800    0x12000    52:4a:93:78:3c:20:00:0a       Yes                7
0x10800    0x12200    52:4a:93:78:3c:20:00:1a       Yes                7
```

We ran the same set of queries with encryption enabled. Even with encryption enabled in flight, the results were very similar to those when encryption was disabled. The only variation was due to the slightly smaller FC frame payload as specified under the FC standards for encryption framing.

Emulex provided performance data on a popular database encryption solution using the same test configuration highlighted previously. Using the same AES-256 level of encryption, the database application struggles to provide the same level of application performance as the HBA due to the added server processing overhead of the software. The TPROC-H benchmark metric of completion time for the 22 database queries is 40% longer for the database application-level encryption, with a significant reduction in disk bandwidth due to the increased application latency.



Overall, it's exciting to see that the Secure HBA encryption has a minimal impact on throughput or latency on an I/O-intensive database workload and is significantly better than the application-based alternative.



Conclusion

As enterprise security threats grow in scale and sophistication, protecting data in motion has become as critical as securing data at rest. Traditional firewall-based defenses and software encryption solutions introduce performance trade-offs that many organizations simply can't afford. The Emulex Secure HBA changes that equation by delivering standards-based, hardware-offloaded encryption that seamlessly integrates into existing servers and Fibre Channel SANs.

In our testing, we found that Emulex Secure HBAs enable in-flight encryption with virtually no performance hit, addressing one of the biggest concerns around EDIF adoption. With encryption fully offloaded to the HBA, storage services like compression and deduplication remain intact, ensuring enterprises don't have to compromise efficiency for security. Even in I/O-intensive database workloads, the impact was negligible—far outperforming traditional software-based encryption methods in both speed and efficiency.

The plug-and-play nature of these HBAs also makes them incredibly easy to deploy, with no significant changes required to the SAN architecture or storage stack. For storage vendors, this is a low-friction, high-value security enhancement that aligns with INCITS FC-SP-3 standards while positioning Fibre Channel for the next era of zero-trust security.

Looking ahead, we expect Emulex Secure HBAs to become a standard layer of SAN security in 2025. With increasing regulatory pressures and the continued rise of ransomware and insider threats, enterprises need robust, transparent, high-performance encryption solutions that don't create new bottlenecks. The Emulex Secure HBA delivers exactly that—a future-proof security upgrade that enterprises can adopt today with confidence.

Brian Beeler , AUTHOR

Brian is located in Cincinnati, Ohio and is the chief analyst and President of StorageReview.com.

This report is sponsored by Broadcom. All views and opinions expressed in this report are based on our unbiased view of the product(s) under consideration.