Emulex SecureHBA Enables Autonomous Fibre Channel SAN Encryption with Everpure FlashArray

AUTHOR
BRIAN BEELER

For the first time, end-to-end, hardware-based in-flight encryption is available across the entire Fibre Channel data path—from server to storage array. Everpure (formerly Pure Storage) is now shipping Fibre Channel-capable FlashArray systems with Emulex SecureHBA technology integrated directly into the array, completing the encrypted transport path the industry has been working toward. Future FlashArray models will ship with SecureHBA as the standard Fibre Channel adapter option. In our evaluation, we assessed the FlashArray//XL130 R5, the first primary storage array to natively bring this capability to the platform.

When SecureHBA-equipped servers connect to the Everpure array, encrypted sessions are established automatically in hardware. There are no additional agents to install and no external encryption infrastructure required. The result is an end-to-end encrypted Fibre Channel connection from server to storage, implemented transparently and without requiring additional software or external encryption infrastructure.

While encryption at rest is standard practice across enterprise storage, encrypting data in-flight, especially within Fibre Channel SAN environments, has been difficult to implement without adding complexity and impacting application performance. Historically, organizations have relied on software-based methods with external key management systems, which introduce additional management overhead and potential risks. Delivering seamless, hardware-level encryption across the storage network has historically been difficult.

Emulex set out to solve that challenge with its SecureHBA. Rather than depending on host software or external systems, SecureHBA performs encryption in hardware, ensuring that application performance and workflows remain unaffected. Since that early coverage, the technology has moved decisively into production. In February, the Fibre Channel Industry Association (FCIA) announced completion of the INCITS Fibre Channel, Security Protocols, Third Edition (FC-SP-3) specification. Emulex SecureHBA is fully compliant with the new standard. SecureHBAs are now widely shipped by major server OEMs, including Dell, HPE, and Lenovo, and more than 120,000 adapters have already been deployed in enterprise environments. In numerous instances, organizations have installed encryption-capable Fibre Channel endpoints during routine server refresh cycles, but haven't fully realized their benefits because the storage arrays lacked native support.

This technical analysis reviews how SecureHBA functions with the tested FlashArray//XL130 R5, examines how Emulex SAN Manager 3.0 provides operational visibility and reporting, and confirms the performance of hardware-based encryption in a real-world setting. A key distinction throughout is where encryption occurs in the data path: unlike application-layer encryption, which renders data incompressible before it reaches the array, SecureHBA encrypts at the Fibre Channel transport layer, preserving array-level compression, deduplication, and ransomware detection capabilities.

Why In-Flight SAN Encryption Matters

Fibre Channel networks have traditionally operated inside a presumed trust boundary. Storage fabrics were physically segmented, tightly managed, and considered insulated from broader network threats. That assumption is increasingly difficult to defend. Ransomware activity remains persistent and adaptive. The Symantec and Carbon Black Threat Hunter Team's Ransomware 2026 report notes that threat actor groups continue to evolve rapidly, with disrupted operations quickly replaced by new affiliates, resulting in sustained year-over-year attack volume. The 2025 Verizon Data Breach Investigations Report corroborates this trend, finding ransomware present in 44% of all breaches analyzed, a 37% increase from the prior year.

These campaigns are infrastructure-aware. Once an attacker gains privileged access, internal lateral visibility becomes possible. While Fibre Channel traffic is not routed like traditional IP traffic, it still operates at the transport layer, moving highly sensitive data between servers and storage. Treating the SAN as inherently secure assumes that perimeter defenses remain intact and that internal compromise never occurs, assumptions that breach patterns increasingly challenge.

The more realistic risk scenario is not an external attacker targeting the Fibre Channel fabric directly, but rather a compromised host or a privileged insider already operating within the environment. When administrative control of a server or virtualization host is obtained, storage traffic moving between the host and the array becomes observable within the infrastructure boundary. Encrypting the transport path ensures that even trusted internal networks do not expose sensitive data during lateral movement or post-compromise activity.

Regulatory expectations are evolving alongside the threat landscape. Frameworks such as CNSA 2.0, NIS2, and DORA place greater emphasis on cryptographic resilience and on protecting data in motion, not just data at rest. Security models are increasingly built around zero-trust principles, where internal network segments are no longer implicitly trusted. As a result, organizations are being pushed to evaluate encryption across all layers of infrastructure, including storage transport paths that were previously assumed to be secure.

There is also an operational dimension. Many modern storage platforms rely on identifying anomalous behavior (such as sudden changes in compression ratios or write patterns) to detect ransomware early. If encryption is applied at the application layer before

data reaches the array, those detection mechanisms can be impaired. Encrypting traffic at the transport layer instead preserves the array's visibility into data characteristics while still protecting it in motion. That architectural distinction becomes increasingly relevant as organizations refine recovery strategies and seek to shorten dwell time during attacks.

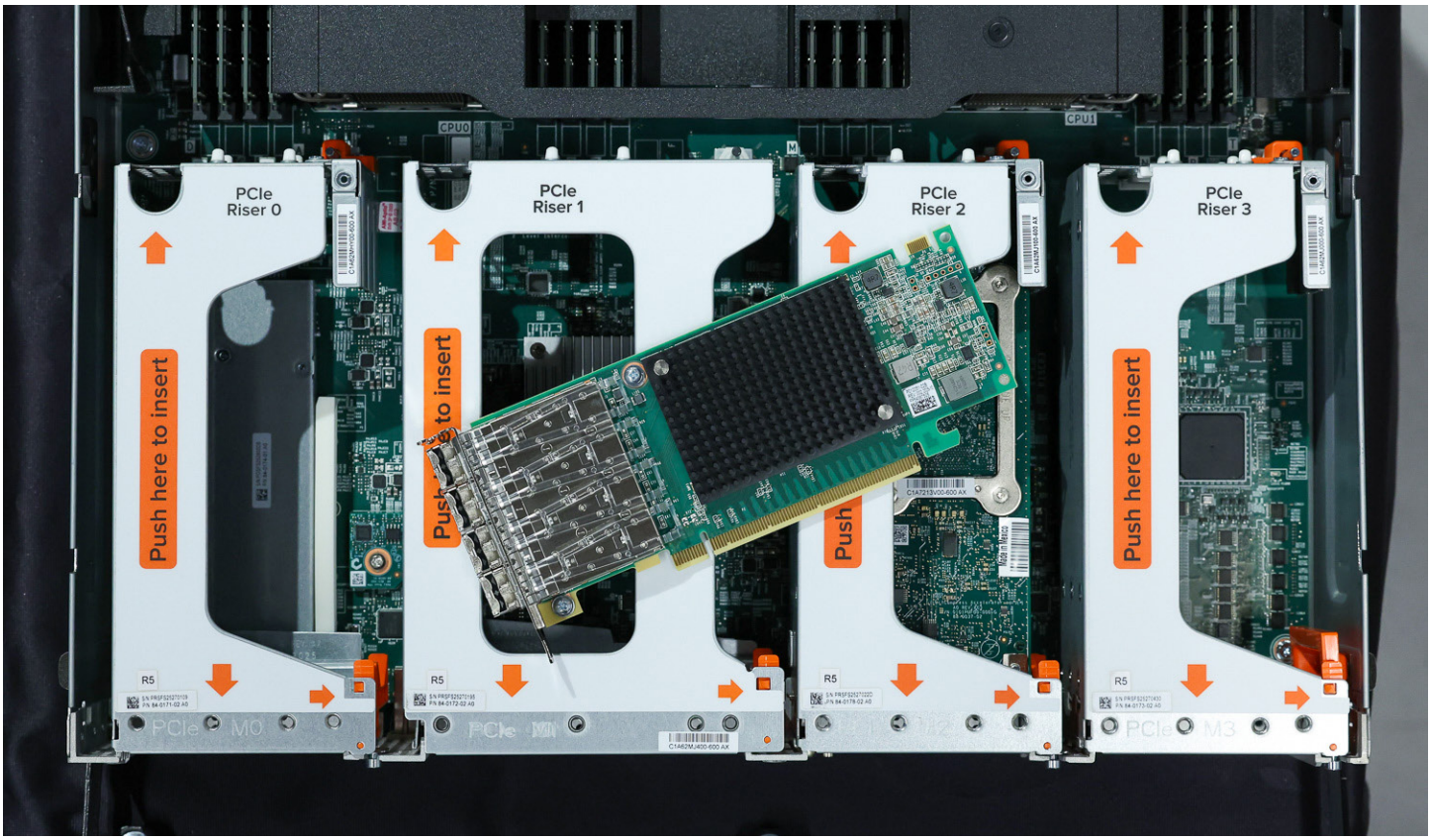
Encryption placement within the data path also affects storage efficiency. When data is encrypted at the application or host level before it reaches the storage system, it typically becomes incompressible because the encryption process removes recognizable data patterns. That can significantly reduce the effectiveness of array-level compression and data reduction services. By contrast, transport-layer encryption within the Fibre Channel stack occurs after data leaves the host but before it traverses the SAN, and is decrypted upon entering the storage array. This approach allows the array to process the original data stream normally, preserving compression, deduplication, and other data services while still protecting the data in flight. The distinction between application-layer and transport-layer encryption is particularly important for organizations that rely on modern storage arrays for efficiency and ransomware detection.

Infrastructure refresh cycles amplify the significance of this moment. Server and storage platforms frequently remain in production for five years or more, meaning the architectural decisions made today shape the security posture for much of the next decade. Encryption capabilities embedded at the hardware level are rarely retrofitted; they are typically selected as part of the foundational design. For organizations evaluating new server deployments or modernizing storage arrays, transport-layer encryption within the SAN should no longer be treated as optional. Hardware-based Fibre Channel PQC-secure encryption represents a durable security control that aligns with evolving compliance expectations, zero-trust models, and long-term risk management.

In-flight SAN encryption is not a reaction to a specific Fibre Channel weakness. It reflects a broader shift in proactive enterprise security thinking: no internal network layer is implicitly trusted, and resilience must be engineered into infrastructure from the outset at every possible level.

SecureHBA Architecture Overview

The Emulex SecureHBA ecosystem is built on the INCITS Fibre Channel Security Protocols, Third Edition (FC-SP-3) standard, providing backward and forward compatibility with existing Fibre Channel networks and adapters. SecureHBAs can be introduced into an existing fabric without requiring switch hardware or software upgrades. When both endpoints support hardware-based encryption, encryption capabilities are negotiated automatically during the standard Fibre Channel login process, and an encrypted session is established without manual configuration.



Because PQC-safe key negotiation is managed entirely by the SecureHBAs, no additional key management infrastructure or operating system configuration is required. PQC-safe, in this context, refers to cryptographic key exchange mechanisms designed to remain resistant to future quantum-computing attacks on traditional public-key algorithms. Session keys are generated and renewed autonomously, allowing encryption to operate transparently within the transport layer.

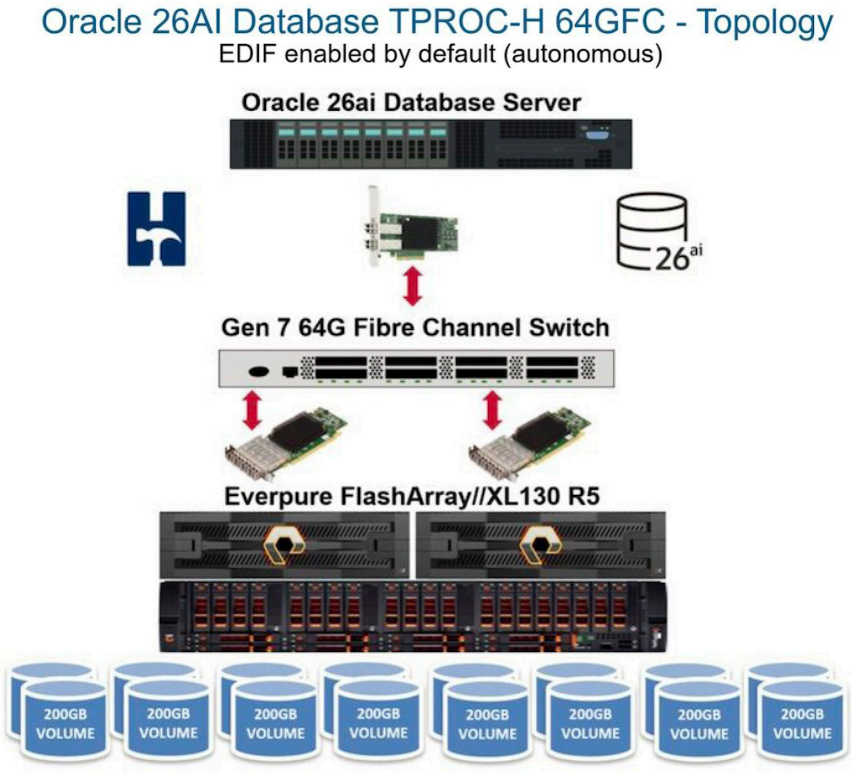
Administrators can change the default behavior, but it's not necessary for full compatibility. An admin may want to change settings to allow only encrypted connections; this will prevent servers that do not support them from connecting. The admin could also disable the feature, allowing all servers to connect without encryption if so desired.
From an architectural standpoint, SecureHBA embeds encryption directly into the Fibre Channel transport path rather than layering it on top of applications or host software. This preserves existing fabric design while enabling in-flight encryption to be deployed without introducing operational complexity.

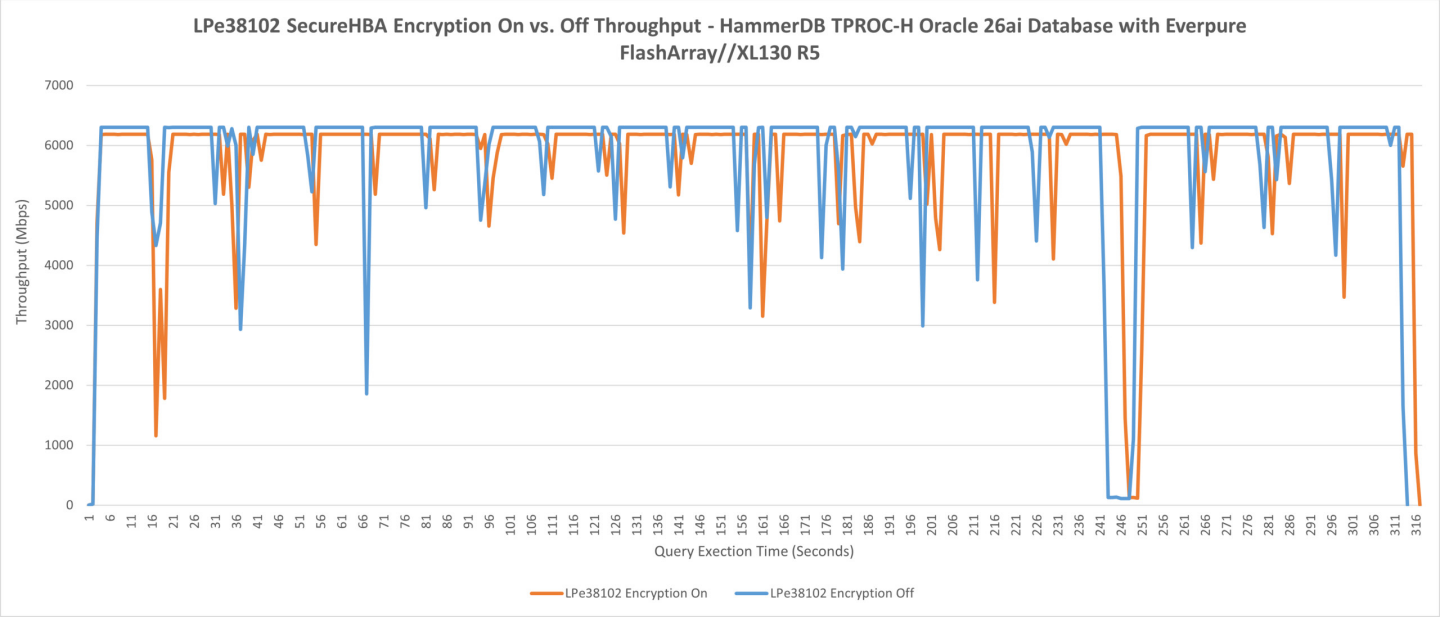
Modern server platforms increasingly include hardware-based trust mechanisms that verify the authenticity and integrity of system components before they engage in production workloads. Technologies such as the silicon root of trust, secure boot chains, and device attestation protocols, including the DMTF Security Protocol and Data Model (SPDM), enable systems to cryptographically verify firmware, adapters, and other devices at startup. These mechanisms ensure that the hardware involved in a workload is genuine and runs with verified firmware before any data transfer begins.

SecureHBA extends the hardware trust model into the storage transport layer itself. Once trusted devices are established at the server and storage endpoints, the encrypted Fibre Channel session protects data in transit between them. In this architecture, identity verification and data protection work together: trusted infrastructure components communicate across an encrypted SAN path without needing additional software layers or external security infrastructure. The result is a security posture that aligns with modern zero-trust principles while maintaining the operational simplicity typical of Fibre Channel environments.

Performance Validation: Oracle TPROC-H Workload

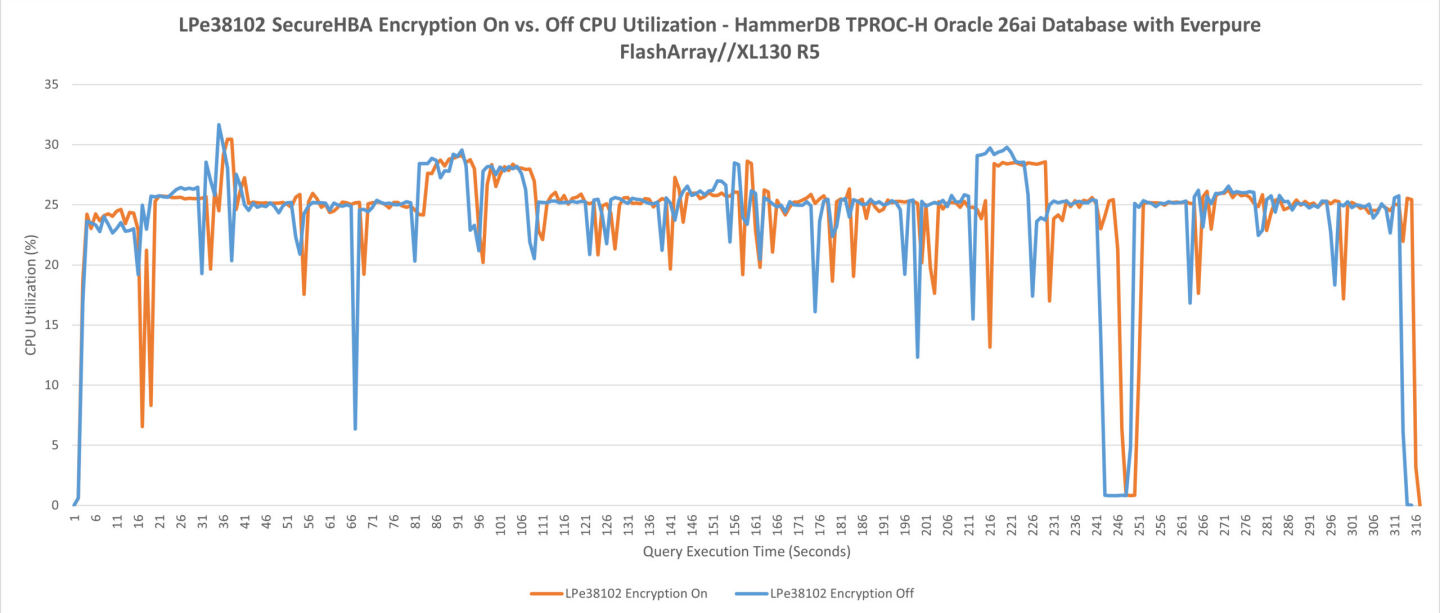
Broadcom and Everpure representatives met with us for a virtual lab session to demonstrate the performance characteristics of unencrypted and encrypted connections using the Emulex SecureHBA and Everpure FlashArray//XL130 R5. The setup consisted of a server with a SecureHBA installed, running Oracle 26ai Database software, with eight 200-gigabyte volumes provisioned on the FlashArray//XL130 R5 for a HammerDB TPROC-H data warehousing test. Designed for maximum throughput, this test allowed us to push the array and SecureHBA to their absolute limits and review their performance with hardware encryption enabled and disabled.





Because software-based encryption solutions impose their penalty directly on the host CPU, the host CPU is the right place to look when evaluating whether hardware offload delivers on its promise. Since all encryption processes occur directly on the SecureHBA's silicon, CPU utilization on the server remained virtually identical across the unencrypted and encrypted test runs. By offloading encryption and decryption to the HBA, data transmission can still occur at maximum throughput without any CPU bottleneck.

Zooming in a bit further, we saw a nearly indistinguishable difference in maximum CPU usage under the TPROC-H workload: 30.46% with an encrypted connection and 31.68% with an insecure connection. Averages for the CPU utilization data were also extremely tight here, with encryption on at 24.35% compared to encryption off at 24.28%. These results are so close that they are well within run-to-run variance and demonstrate that the SecureHBA's onboard encryption processes do not affect host CPU usage.



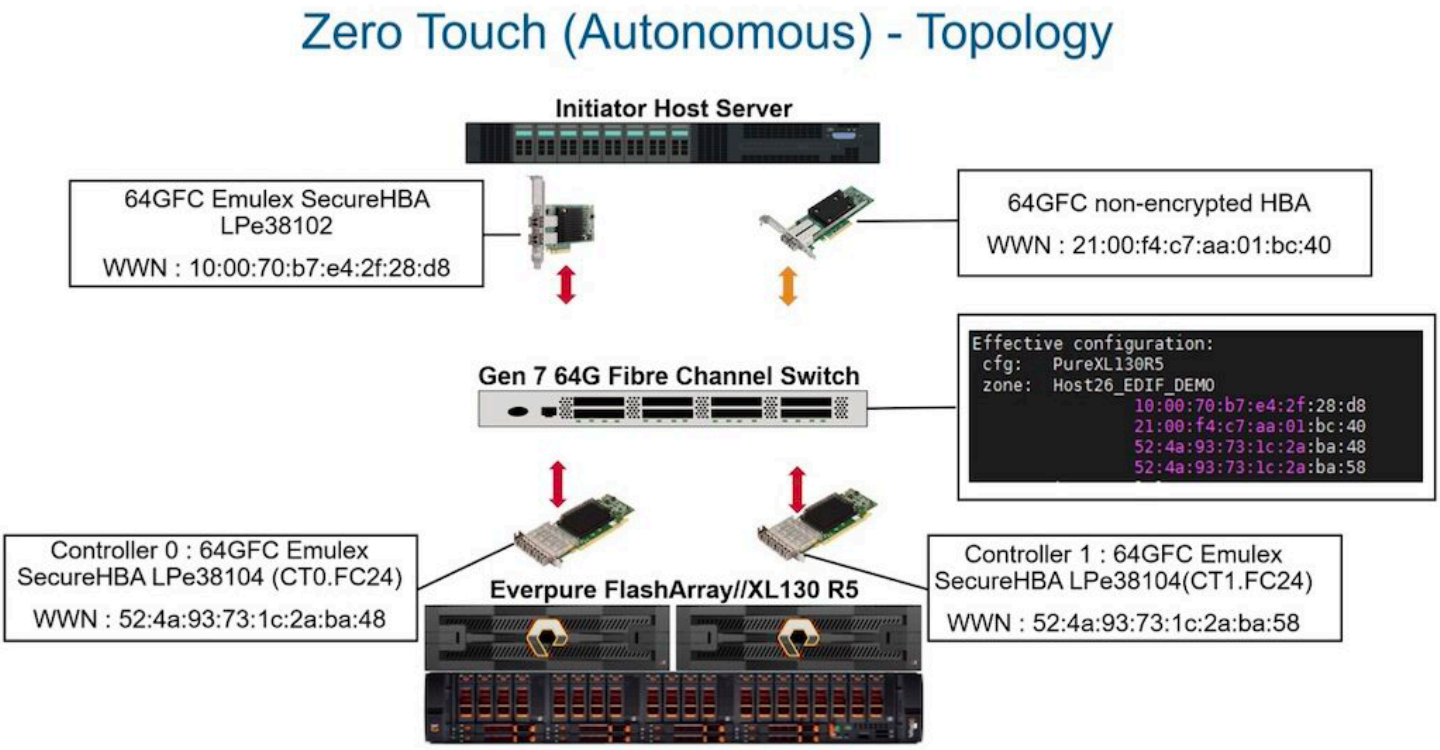
When using solutions that depend on key manager servers or services, both the active and passive sides of the connection must be configured and tested to ensure proper authentication and encryption, as well as successful failover. Since Emulex performs this automatically in hardware, it isn't a concern for administrators. For alternative solutions that depend on external key manager services, both active and standby paths must be individually configured, authenticated, and validated to ensure proper failover behavior.

In large SAN environments with thousands of connections, the time and operational complexity required to verify those paths can increase significantly. This process could involve thousands of connections per port and might significantly extend the overall duration. By handling encryption negotiation directly within the SecureHBA hardware, these additional authentication steps are eliminated, minimizing the risk of misconfiguration or delayed failover. Additionally, solutions that rely on external key managers risk misconfiguration or out-of-sync certificates across all connections, including the passive path. This may not be immediately obvious, since most connectivity issues are only noticed when the active path encounters a problem.

With Everpure's FlashArray//XL130 R5 and SecureHBAs, customers can expect a rapid, secure cutover during critical failures, thanks to its resilient dual-controller architecture and autonomous encrypted connection re-establishment. When storage fabrics fail, Everpure and Emulex allow administrators to focus on the underlying issue, with SAN failover handled automatically in the background.

Operational Validation: How Encryption Is Observed in Practice

During our lab session, Emulex gave us a quick demonstration of their zero-touch provisioning feature using the Emulex SecureHBA. This lab's hardware topology consisted of an initiator host server with two HBAs: one 64G Fibre Channel SecureHBA and one 64G Fibre Channel HBA without hardware encryption features. Both initiators were connected to an Everpure FlashArray//XL130 R5 with two SecureHBAs configured as targets.



Using the command-line interface on the XL130 R5, Everpure showcased seamless, automatically encrypted connections and showed exactly how the encryption status of each port is displayed, as pictured below.

```
tme@ECD-IRV-FA-XL130R5-ct1:~$ pureport list --init | grep -i 10:00:70:B7:E4:2F:28:D8
10:00:70:B7:E4:2F:28:D8  -                    -             -              CT0.FC24  52:4A:93:73:1C:2A:BA:48  -  -  -  -  HW Encrypted
10:00:70:B7:E4:2F:28:D8  -                    -             -              CT1.FC24  52:4A:93:73:1C:2A:BA:58  -  -  -  -  HW Encrypted
tme@ECD-IRV-FA-XL130R5-ct1:~$ pureport list --init | grep -i 21:00:F4:C7:AA:01:BC:40
21:00:F4:C7:AA:01:BC:40  -                    -             -              CT0.FC24  52:4A:93:73:1C:2A:BA:48  -  -  -  -  -
21:00:F4:C7:AA:01:BC:40  -                    -             -              CT1.FC24  52:4A:93:73:1C:2A:BA:58  -  -  -  -  -
tme@ECD-IRV-FA-XL130R5-ct1:~$
```

The Everpure CLI can also reveal more detailed encryption information from SecureHBAs, including whether the connection uses post-quantum cryptography and the HBA's re-keying deadline.

```
[root@HOST26-R770-RHEL9 DEMO]# hbacmd getconnectioninfo 10:00:70:b7:e4:2f:28:d8

                                                    Post-Quantum      Days Until
   S_ID       D_ID          Peer WWPN               Cryptography       Rekey
---------- ---------- ------------------------  ----------------   -----------
0x11900    0x10100    52:4a:93:73:1c:2a:ba:48        Yes                6
0x11900    0x10400    52:4a:93:73:1c:2a:ba:58        Yes                6
```

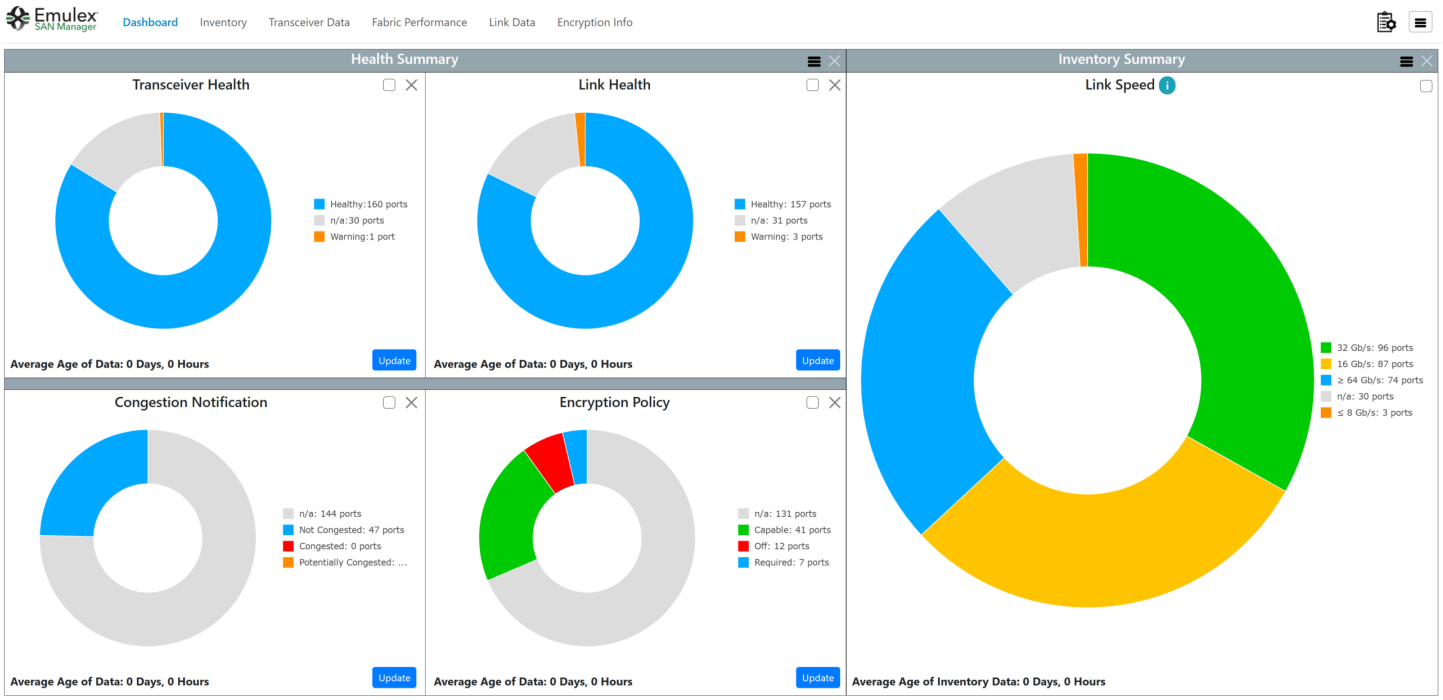
By default, encrypted connections were immediately established between the SecureHBAs on the initiator host server and the Everpure FlashArray//XL130 R5. An unencrypted connection was established between the standard Fibre Channel HBA and the same array port, demonstrating ease of use while maintaining broad compatibility.

Emulex SAN Manager 3.0: Fabric-Level Visibility and Compliance

Highlights and New Features

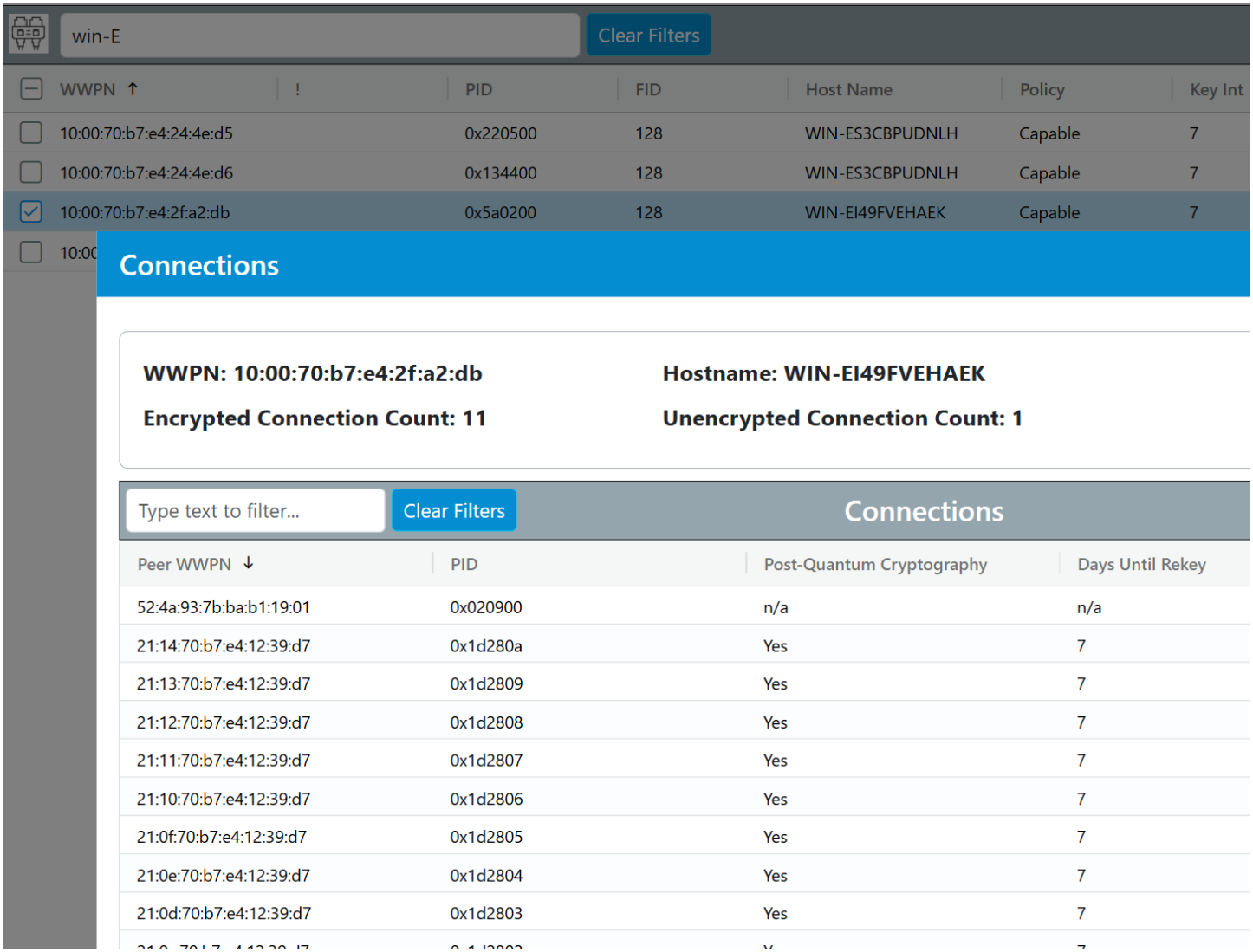
- **Quick access to the encryption status of every connection in a SAN**
- **Built-in reporting tools for auditing and evaluating SAN-wide security compliance**
- **Scripting-friendly platform with a Python-based CLI and automatic event notification via SMTP**

For customers using Emulex Fibre Channel HBAs (including SecureHBAs), Broadcom offers Emulex SAN Manager 3.0 software at no additional cost. Since its inception in 2020, the software has been designed to give storage administrators deeper insight into their SAN and to provide tools for monitoring, maintenance, and reporting across multiple Fibre Channel environments. Upon login, clear doughnut-style charts provide an overview of SAN-wide performance and health data using widgets that can be customized and rearranged to suit the user's preferences. Each one of these widgets can be clicked on to reveal the data behind each chart.



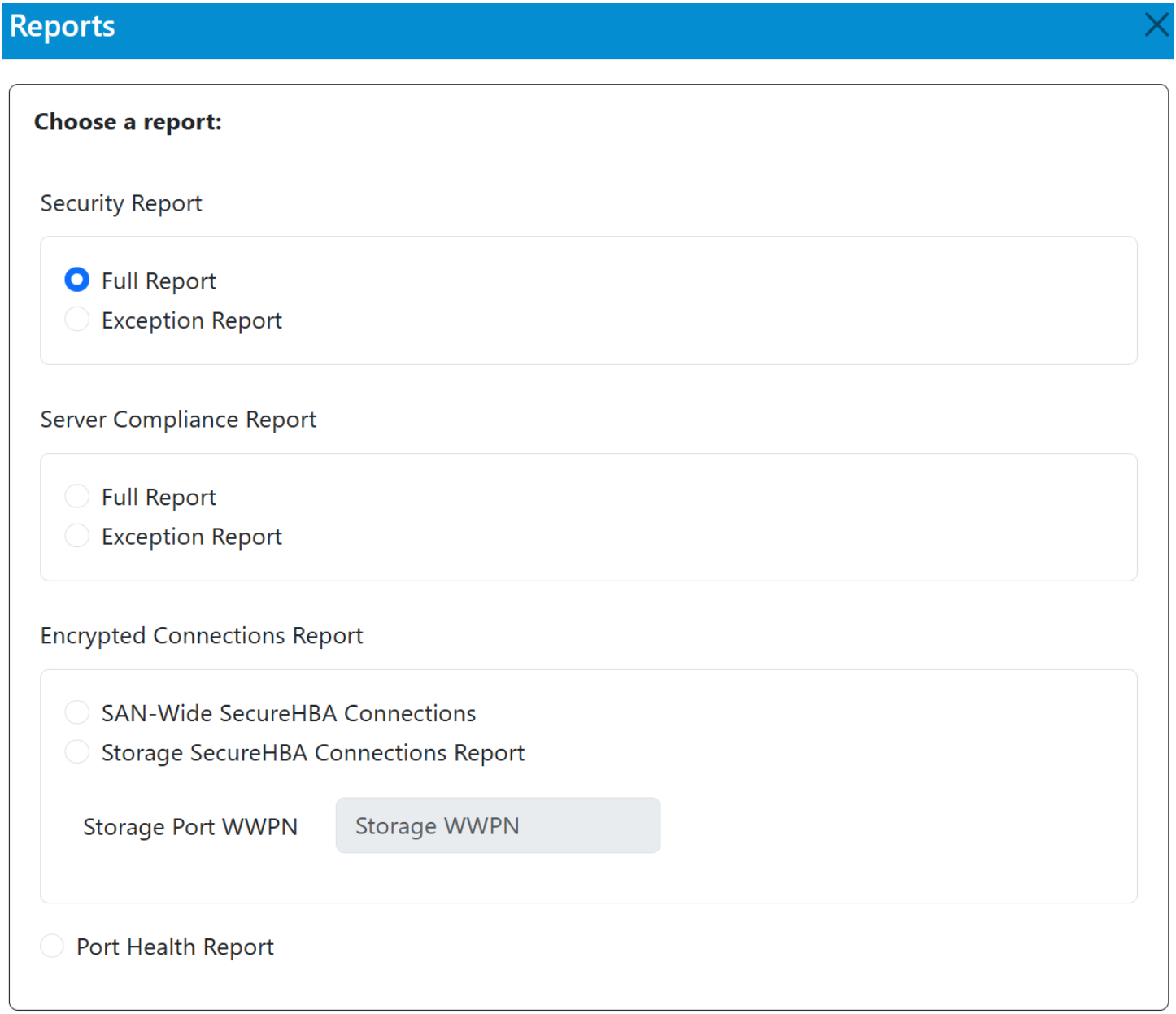
Released alongside the Emulex SecureHBA are new features in SAN Manager 3.0. Users can now use the "Encryption Policy" widget on the dashboard to see exactly how many Emulex Fibre Channel nodes are capable of encryption, have encryption required, or have encryption capabilities turned off.

Clicking on the "Encryption Policy" widget or the "Encryption Info" header in SAN Manager 3.0 provides a detailed list of all connected ports, which can be filtered and sorted by attributes such as WWPN, Host Name, Policy, and Key Interval. This makes it easy to find and manage ports quickly, and it can provide even more information when a specific port is selected.



In addition to viewing configured encryption policies in the dashboard, Emulex SAN Manager 3.0 now includes built-in reporting tools for auditing and compliance verification. CSV-formatted security reports can now be generated and exported (via download or email) directly in the application, saving busy IT managers the hassle of gathering information from potentially thousands of Fibre Channel nodes and manually verifying compliance.

WWPN	PID	F	Host Name	Model	Encryption Pol	Rekey Inter	Encrypted Connectic	Unencrypted Connectic	FW/Driver Sta	Exceptions	Notes
10:00:70:b7:e4:13:bd:94	0x1d1e00	128	config17	LPe38102	OFF	7	0	3	n/a	Encryption Disabled	
10:00:70:b7:e4:0d:5b:42	0x1b1f00	128	config1	LPe38100	OFF	7	0	0	n/a	Encryption Disabled	
10:00:70:b7:e4:24:4e:d6	0x134400	128	WIN-ES3CBPUDNLH	LPe38102-D	Capable	7	0	4	Outdated	Outdated FW/Driver Version	Rec FW: 14.4.730.7, Rec driver: 14.4.624.1
10:00:70:b7:e4:24:61:b7	0x221c00	128	WIN-T9J3U3FR9NN	LPe37102-D	Capable	7	0	0	Outdated	Outdated FW/Driver Version	Rec FW: 14.4.730.7, Rec driver: 14.4.624.1
10:00:70:b7:e4:24:61:b8	0x221f00	128	WIN-T9J3U3FR9NN	LPe37102-D	Required	7	0	0	Outdated	Outdated FW/Driver Version	Rec FW: 14.4.730.7, Rec driver: 14.4.624.1
10:00:5c:ba:2c:fc:39:2b	0x1b0900	128	discovery1	SN1620E2P	Capable	7	1	0	Outdated	Outdated FW/Driver Version	Rec FW: 14.4.731.5, Rec driver: n/a
10:00:70:b7:e4:24:4e:d5	0x220500	128	WIN-ES3CBPUDNLH	LPe38102-D	Capable	7	0	8	Outdated	Outdated FW/Driver Version	Rec FW: 14.4.730.7, Rec driver: 14.4.624.1



The Emulex SAN Manager also provides users with visibility into their SAN health, with tools to moderate congestion, identify failing transceivers, and view link speeds. In addition to being an excellent GUI-based tool, Broadcom has created opportunities for automation-minded IT folks with a Python-based command-line interface for scripting. It plans to add built-in webhooks that analysts can use to export and review performance and reliability data from the SAN Manager to other applications and tools for review. Even email alerts (via SMTP) that warn administrators of critical events can be configured using a powerful task scheduler. Driven mainly by customer requests, the development team is working hard to make the application an extensible, all-in-one platform. Emulex SAN Manager 3.0 will be a welcome addition to any storage administrator's arsenal when an Emulex SAN's encryption compliance, health, multipathing, or performance needs to be reviewed.

Final Thoughts

The Everpure FlashArray with Emulex SecureHBA represents the first production deployment of transport-layer, PQC-safe encryption across the Fibre Channel data path.

The introduction of hardware-based, transport-layer encryption into the Fibre Channel stack marks a meaningful shift in how enterprises think about storage security. For years, Fibre Channel fabrics operated inside an implicit trust boundary. Emulex

SecureHBA challenges that assumption by embedding encryption directly into the transport layer, without altering fabric design or introducing operational overhead. Our evaluation of the Everpure FlashArray with Emulex SecureHBAs demonstrates that end-to-end, in-flight encryption can be deployed without measurable performance degradation or added complexity. Encryption was negotiated automatically, scaled across more than one thousand sessions, and preserved the array's data

Emulex has already established a significant footprint, with more than 120,000 SecureHBAs shipped across major server OEM platforms. The addition of a storage array endpoint closes the loop, enabling true end-to-end encryption across the SAN. While Everpure is the first to integrate SecureHBA at the array level, the architectural approach is standards-based and positioned to extend across future Fibre Channel platforms as hardware refresh cycles continue.

Because this solution is standards-based, it ensures interoperability. Although Emulex and Everpure are the first to introduce it, it still leaves room for interoperability between other brands' HBAs and storage arrays. This solution is fabric-agnostic and can seamlessly extend to fabric extension solutions (FC-IP). Since everything is managed in hardware, the solution does not require specific software versions or additional OS version-specific feature packages.

Infrastructure decisions made today often define enterprise risk posture for the next five to seven years. As organizations modernize servers and storage arrays, embedding PQC-safe encryption at the transport layer provides a durable security control that aligns with evolving compliance expectations and zero-trust principles. SecureHBA positions in-flight SAN encryption as a foundational element of modern Fibre Channel design, aligning security, performance, and operational simplicity within the transport layer itself.

Brian Beeler

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