Mice

Enterprise Strategy Group

SHOWCASE

NOVEMBER 2025

Building a Quantum-safe SAN for the Enterprise AI Era

Scott Sinclair, Practice Director; and Monya Keane, Senior Research Analyst

Abstract: It is critical for enterprises to both protect valuable data (the lifeblood of the business) and ensure business continuity, which requires the availability and performance of critical applications. Post-quantum cryptography, part of Brocade Gen 8 SAN technology, is addressing a new but essential requirement for storage environments. The emergence of the era of enterprise AI is also placing even greater demands and requirements on the storage systems servicing the enterprise data, meaning businesses must place an even greater priority on modernization.

Introduction

An imperative exists among enterprise organizations to modernize their on-premises infrastructures to serve multiple purposes—for example, to simplify operations and support business growth, support a new wave of enterprise private AI initiatives, and enhance security. IT decision-makers regard security as a key driver for delivering business value. They proactively want and need to select products that can deliver the necessary levels of security today and in the future without sacrificing or impacting business goals and the IT infrastructure's agility.

According to research by Enterprise Strategy Group, 84% of IT decision-makers agreed that data center modernization is a top IT priority.[1] There has also been a move away from cloud data centers and back to on-premises storage due to the need for data sovereignty. More than one in four IT decision-makers (27%) identified strengthening cybersecurity tools and processes as the single most important IT initiative for their organization. It was the most common response and outpaced artificial intelligence nearly two to one as the top IT priority (27% versus 16%).[2]

The need for superior security and resilience fuels new infrastructure investments, including those to support private enterprise AI. Increased resilience against cyberthreats is also a must-have to reduce business risk, and it must be a priority as organizations demand higher performance with greater access to data.

Of note as well is that enterprise data center attack surfaces will continue to grow aggressively. The percentage of bot traffic represented almost 50% of total internet traffic for the first time ever in 2024, and 37% of internet traffic was tied to malicious bots.[3] Coupled with more than 50,000 common vulnerabilities and exposures last year, organizations have no choice but to upgrade the security of their environments. Not to do so is tantamount to becoming the "weak member of the herd."

Also arising is the issue of quantum computing. Strengthening cybersecurity is an even more essential task with the pending entrance of quantum computing, which is poised to become a reality within the next few years. The rise of accessible quantum computing could introduce serious threats to traditional encryption and cybersecurity practices. As a result, quantum-safe protection is going to be a must-have capability. Any infrastructure modernization effort

[1] Source: Enterprise Strategy Group Research Report, *Private AI, Virtualization, and Cloud: Transforming the Future of Infrastructure Modernization*, July 2025.
[2] Source: Enterprise Strategy Group Research Report, *2025 Technology Spending Intentions Survey*, December 2024.
[3] Source: 2024 Bad Bot Report.

that does not incorporate quantum-safe protections such as encryption will likely have a short-life span, ultimately increasing business risk and reducing ROI.

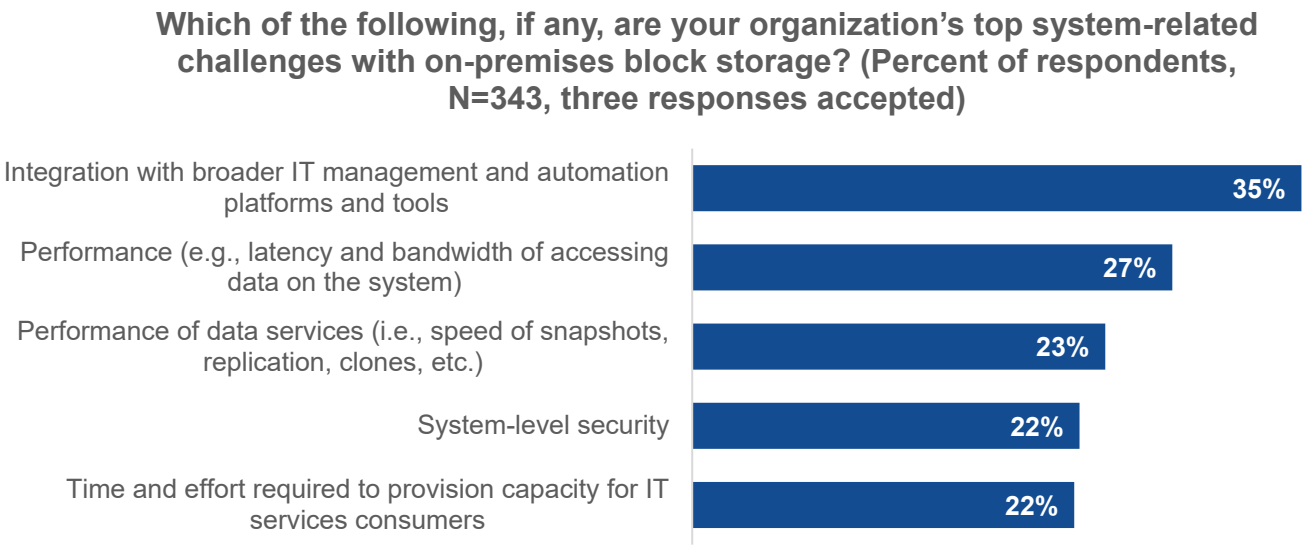
Fortunately, IT industry leader Broadcom is responding to this new need by introducing Brocade Gen 8, with support for quantum-safe encryption.

Data Security Enhancements Must Underpin Storage Modernization

Enterprise Strategy Group research highlights the rise of on-premises storage modernization efforts, especially to improve cyber resilience. Among IT organizations with a new on-premises storage infrastructure project either active or planned for the near-term (i.e., in the next six months), 46% identified the need to better protect against security threats as a core initiative driving their storage investments.[4] And 86% of organizations agreed that improving storage-based security is key to strengthening their overall security posture.[5]

Figure 1 illustrates the top storage challenges identified by IT decision-makers. The importance of performance (27%) and security (22%) are two primary concerns.[6]

Figure 1. Five Most Common SAN Challenges



Source: Enterprise Strategy Group, now part of Omdia

Again, the rise of quantum computing and its pending impact on cybersecurity is beginning to affect how businesses should approach infrastructure modernization. They should know that in 2022, the U.S. National Security Agency (NSA) published the Commercial National Security Algorithm 2.0 advisory, which urged companies to plan, prepare, and budget for an effective transition to quantum-resistant (QR) algorithms. And in 2024, the U.S. National Institute of Standards and Technology (NIST) released an Initial Public Draft report detailing its roadmap for post-quantum cryptography adoption. That report includes aggressive timelines for deprecating (by 2030) and disallowing (by 2035) a broad range of currently used security algorithms.[7]

[4] Source: Enterprise Strategy Group Research Report, *Navigating the Cloud and AI Revolution: The State of Enterprise Storage and HCI*, March 2024.
[5] Source: Enterprise Strategy Group Research Report, *The Critical Role of Storage in Building an Enterprise AI Infrastructure*, September 2025.
[6] Ibid.
[7] Source: "Transition to Post-Quantum Cryptography Standards," NIST.gov, November 2024.

Given the longevity of data storage and the cost of storage network infrastructure investments, it is important to ensure that any new investment can not only support performance, availability, and scale requirements but can also provide a path to ensuring the highest level of security for the long term. According to Broadcom, most organizations can only refresh 20% of their application footprint in a given year (although the pace of application refreshment is highly variable and depends on several factors). Therefore, it is vital to begin the process now to meet the 2030 timeline and ensure that storage investments (1) adhere to NIST requirements and (2) improve security, given the expected continued rise of AI initiatives.

Ninety-two percent of organizations are either actively pursuing or exploring private, enterprise AI initiatives that feature the augmentation, tuning, or training of AI models on premises with private data.[8] Without a proper storage infrastructure offering high levels of cyber resilience, security, and performance, AI initiatives will fail. Enterprise Strategy Group found that 83% of IT decision-makers agreed that success in AI is impossible if the data is not secured and protected.[9]

Notably, 83% of organizations also expected to upgrade their storage environment in the next 24 months to support growing AI demands.[10] Consider that one industrial espionage gambit is to poison the learning stream of an AI inference engine. It is already being done by bots on social media. It is, thus, unsurprising that a large majority of storage decision-makers (87%) said AI is driving substantial data growth, and a similarly large percentage (79%) said AI is presenting them with significant data security challenges.[11]

Broadcom Brocade Gen 8 With Post-quantum Cryptography

Broadcom Brocade Gen 8 technology already meets the NIST recommendation, giving enterprises time (by starting now) to implement and/or migrate to a quantum-safe infrastructure while delivering on all the requirements of the enterprise AI era.

Broadcom designed Brocade Gen 8 technology to deliver the performance, automation, and security necessary for data-intensive, mission-critical enterprise applications, including artificial intelligence initiatives, thereby taking the autonomous SAN to the next level. For example, the Brocade X8-8 Director, the Brocade X8-4 Director, and the Brocade G820 Enterprise Switch offer improved low-latency performance and higher levels of throughput. Gen 8 technology also includes:

- Integrated, AI-powered SAN management technology for autonomous operation and improved performance consistency for applications.
- SAN Fabric Intelligence to eliminate time-consuming, manual correlation of all application resources to drill down into points of interest to accelerate troubleshooting and to drive smarter management decisions.
- An Adaptive Traffic Optimizer that learns and adapts to changing application demands by dynamic load balancing across virtual channels.
- 128G and low latency to maximize VM and application density for unmatched efficiency and utilization and to build scalable and efficient fabrics by using fewer chassis and switches.
- Self-healing capabilities to maintain uptime if/when issues arise.
- Integrated security with quantum-resistant encryption and embedded SAN AI technology to safeguard SAN fabrics against cybersecurity threats in the era of quantum computing.

---

[8] Source: Enterprise Strategy Group Research Report, *Private AI, Virtualization, and Cloud: Transforming the Future of Infrastructure Modernization*, July 2025.

[9] Source: Enterprise Strategy Group Research Report, *IT Transformed: Inside the Convergence of Hybrid Cloud and AI*, July 2025.

[10] Source: Enterprise Strategy Group Research Report, *The Critical Role of Storage in Building an Enterprise AI Infrastructure*, September 2025.

[11] Ibid.

It's also important to keep in mind the inherent cybersecurity benefits of Fibre Channel technology. Unlike any-to-any network traffic, Fibre Channel storage traffic is isolated through zoning, enforcing point-to-point access to assign storage targets directly to hosts and protect against unauthorized access.

According to Enterprise Strategy Group research, 51% of storage administrators who expect Fibre Channel to be their dominant storage network architecture moving forward credited superior security as a top factor driving that decision.[12]

With Fibre Channel, it is possible to encrypt all traffic in flight without performance degradation while continuing to take advantage of the storage array's data reduction technologies. Organizations that leverage Brocade Fibre Channel SAN and Broadcom Secure HBAs can securely move data encrypted between servers and storage, without impacting the storage system's data efficiency capabilities such as dedupe or compression (thanks to the storage system's data reduction capabilities) with subsequent data at rest encryption. Plus, it all works automatically and does not require any configuration.

Brocade's Fibre Channel SAN architecture also minimizes attack surfaces with its strong access controls and limited privileges based on an industry best practice (Principle of Least Privilege) architecture. Locking down access strengthens overall system security and reduces potential exposure to security breaches, accidental errors, and intentional misuse of privileges. Brocade's Fabric OS also provides a centralized view, enabling administrators to verify that all traffic in the fabric is encrypted. Additionally, Brocade monitors and alerts IT about security configuration changes and events.

The switch uses quantum-resistant algorithms and is designed to be resistant to quantum attacks, thereby protecting sensitive data and critical infrastructure from being decrypted by future quantum computers.

The goal of these advances is to protect SAN fabrics against attacks with advanced cryptographic algorithms, while reducing the risk of malicious software being installed with digitally signed firmware and software. Support for post-quantum cryptographic algorithms includes ML-DSA (Module-Lattice-based Digital Signature Algorithm), ML-KEM (Module-Lattice-based Key-Encapsulation Mechanism), LMS (Leighton-Micali Signature), and others.

Security enhancements such as those will better protect organizations against future threats associated with quantum computing. While the threats might not yet be immediate, the longevity of SAN networks necessitates near-term action. That is why it is such good news that Brocade technology already adheres to NIST recommendations today. Brocade engineering foresight is giving enterprises time to implement and migrate to a Quantum Safe infrastructure while delivering on all the requirements of the enterprise AI era. Again, because most businesses can or will only migrate a small portion of their environments at any given time, the time to start is now.

Conclusion

The convergence of enterprise AI adoption and looming quantum computing-related threats creates an unprecedented imperative for storage infrastructure modernization. With 92% of organizations pursuing private AI initiatives, and quantum computing poised to render current encryption at least partially obsolete by 2030, the window for proactive infrastructure transformation is already starting to close.

The reality is that traditional approaches to storage security are insufficient for the challenges ahead. The growth of attack surfaces, the rise of malicious bot traffic, and the NIST mandate for post-quantum cryptography adoption by 2030 collectively demand immediate action from enterprise IT leaders.

Broadcom's Brocade Gen 8 technology with post-quantum cryptography represents more than an incremental upgrade—it is a strategic investment in long-term business continuity. By delivering quantum-resistant encryption,

[12] Source: Enterprise Strategy Group Research Report, *Navigating the Cloud and AI Revolution: The State of Enterprise Storage and HCI,* March 2024.

AI-powered autonomous management, and the inherent security advantages of a Fibre Channel architecture, this solution addresses both current operational demands and future security requirements in a single platform.

The organizations that act decisively today will secure a competitive advantage through superior data protection, AI-ready performance, and secure infrastructure. Conversely, those that delay risk becoming vulnerable in an increasingly hostile cyber landscape. The choice is clear: invest in a quantum-safe storage infrastructure now, or face potentially catastrophic consequences when quantum computing becomes mainstream reality.

Brocade Gen 8 serves as the foundation for enabling a business to thrive in the era of enterprise AI and avoid cyber threats associated with quantum computing—all while fulfilling both current and future requirements.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com