

The AI Threat-Secure, Quantum-Safe Storage Fabric



Fortify Your Data Assets on the Most Secure Network in the Data Center

Legacy networks cannot contain frontier agentic AI tools that exploit and move laterally at machine speed, nor do they comply with mandates for quantum-resistant infrastructures. To protect your mission-critical data, your storage must reside on an unassailable foundation.

Fibre Channel has always been the most secure network in the data center. Brocade® FOS 10AI and next-generation Gen 8 Fibre Channel delivers an impenetrable high-performance storage fabric. The network architecture combines AI Threat-Secure defense with quantum-safe cryptography to fortify your most critical data assets today and tomorrow.

The Compounding Threat: Frontier AI and Quantum Decryption

Autonomous AI tools can launch nonstop, automated attacks that learn and exploit undetected vulnerabilities. Left unchecked, these intelligent agents can silently exfiltrate vast volumes of critical data for future decryption. By pairing an AI Threat-Secure network architecture with quantum-safe cryptography, Brocade Fibre Channel ensures a complete defense lifecycle and strengthens cyber resilience against sophisticated, next-generation security risks.

- **Neutralize frontier AI threats:** Reduce the attack surface by ensuring vulnerabilities across the fabric are continuously identified, isolated, and remediated before autonomous bots or malicious actors can exploit them.
- **Defeat post-quantum threats:** Protect data in-flight with built-in post-quantum cryptography and end-to-end encryption, safeguarding sensitive assets against "harvest now, decrypt later" exploitation.

Architectural Advantages in SAN Security

This defense is built upon the most secure network in the data center for a reason. Traditional data center IP/Ethernet networks are inherently routable, highly interconnected, and plagued by a sprawling attack surface exposed to lateral breach contagion. Fibre Channel is a completely non-routable, dedicated storage network. This architectural isolation means that Brocade fabrics remain structurally invisible to network-layer threat actors and autonomous scanning tools. Layering AI Threat-Secure and quantum-safe defenses onto this isolated, AI-fortified architecture creates a foundation that is structurally unassailable by today's adversarial AI and tomorrow's quantum technology. The result is an isolated, self-defending storage environment that shields your SAN against autonomous AI threats and post quantum computing risks, meeting the strictest compliance standards without adding operational complexity.

The Brocade Multi-Layered Defense

AI-Threat-Secure FOS 10AI Software

Brocade FOS 10AI delivers the purpose-built, continuously hardened operating system designed to stay ahead of modern exploits. Each major release integrates advanced frontier agentic AI scanning and multi-layer threat detection across the OS, application, and open-source stacks to identify and neutralize vulnerabilities before code ever touches production infrastructure. In addition, the operating system undergoes rigorous internal and independent third-party penetration testing. Real-time monitoring of global threat databases paired with a rapid patching process ensures newly discovered zero-day risks are mitigated immediately.

Quantum-Safe Gen 8 Hardware

Brocade Gen 8 hardware delivers a quantum-safe foundation engineered to withstand both immediate and long-term security threats. By integrating post-quantum cryptography directly into the platform, it safeguards mission-critical data against post-quantum computing threats. Additionally, enhanced anti-tampering technology locks down the hardware at the silicon level to block unauthorized modifications and eliminate malicious code installation.

Brocade Fabric-to-Silicon Security Guardrails

Continuous Posture Management

Automated security assessments and real-time fabric visibility (via Brocade Fabric OS® software and Brocade SANnav™ software) eliminates blind spots, enforces compliance and instantly alerts unauthorized changes.

Proactive Threat Mitigation

Frontier agentic AI scanning and automated penetration testing isolates and patches vulnerabilities, while integrated post-quantum cryptography fortifies data against emerging threats.

Hardware and Software Validation

Silicon Root of Trust and TruFOS Certificates continuously verify authenticity to prevent counterfeit hardware or rogue firmware.

Hardened Attack Surface

Strict principle-of-least-privilege access controls and the elimination of root-level accounts stops exploits in their tracks.

Physical Isolation

Non-routable, point-to-point architecture inherently segments storage traffic, removing vulnerabilities common to IP networks.

Learn More

The time to fortify your storage network is now. Can you afford the risk of not doing so? Explore the Brocade Gen 8 webpage to see how next-gen Fibre Channel secures, automates, and powers your SAN.

[View Webpage](#)