Future-Proof Against Emerging Post-Quantum Threats

With Cloudflare and Accenture, you can protect data from both existing and novel threats while addressing compliance standards

Protection for today and tomorrow

Encryption's quantum deadline is here

Quantum computers pose a serious threat to current encryption standards, potentially breaking the cryptography methods used for Internet security today. Sensitive information is at risk of "harvest now, decrypt later" threats where adversaries steal encrypted data to decrypt it once quantum computing matures.

Not only must encryption evolve to protect data from these attacks, but NIST has announced plans to deprecate current encryption standards by 2030 and completely disallow them after 2035. With typical enterprise cryptography migrations taking 5-10 years, the time to begin implementing post-quantum cryptography is now.

Preparing for the post-quantum future

Organizations need resilient cryptographic solutions that can withstand both current and emerging quantum threats without disrupting existing operations. This requires a flexible framework that can adapt to evolving standards while maintaining network performance and compatibility with existing systems.

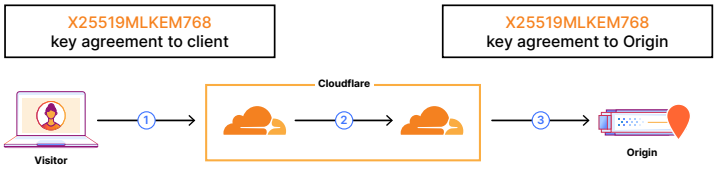

Figure 1: Cloudflare's quantum-safe CDN

Secure traffic with post-quantum hybrid key agreements using Cloudflare.

Quantum-safe encryption is available now

To address the immediate need for post-quantum security, Cloudflare and Accenture are working together to help organizations navigate the transition. This partnership unites Accenture's security advisory services and implementation expertise with Cloudflare's global network featuring quantum-resistant encryption capabilities.

Cloudflare's content delivery network (CDN) delivers quantum-safe encryption by default across its vast global network, with over 35% of connections already using post-quantum hybrid key agreements. By taking an iterative approach, Cloudflare and Accenture can offer low-risk migration that provides **immediate security without configuration changes**. End-to-end quantum security protects traffic from the end client to the Cloudflare edge and between Cloudflare and the origin server while maintaining performance.

Future-proof security

Protect against "harvest now, decrypt later" attacks by deploying quantum-resistant encryption today.

Zero-effort implementation

Enable post-quantum encryption with no additional configuration or performance impact.

End-to-end protection

Safeguard all traffic from users to origin servers, ensuring data protection against both existing and future threats.

Unified security and encryption

Encryption alone is an incomplete security strategy. Cloudflare's security stack includes DDoS protection, Web Application Firewall, API Gateway, and bot management solutions that work in concert with the quantum-safe CDN to provide comprehensive protection against both current and future threats. Post-quantum cryptography support is also available in Cloudflare's secure web gateway to block threats in TLS traffic.

Quantum-safe Zero Trust Network Access

In the near future, organizations will be able to protect Internet traffic traveling to any corporate office, cloud environment, or data center. Cloudflare's WARP client installed on end users' devices will provide quantum-resistant VPN replacement using WARP-client-to-tunnel network configurations.

Developing the future of authentication, certificates, and PKI

Over the next one to two years, post-quantum encryption will likely see significant integration into authentication, certificates, and Public Key Infrastructure (PKI). Cloudflare is at the forefront of these developments, contributing to post-quantum cryptography research, implementation, and standardization. Efforts include collaboration with academic and industry partners, participation in NIST and IETFA standardization processes, supporting open source cryptographic libraries, testing post-quantum TLS in its infrastructure, publishing educational content, and developing transition tools.

Experienced quantum security guidance

Accenture works with Cloudflare to help organizations navigate the complex transition to quantum-safe infrastructure. Through strategic advisory services, Accenture conducts enterprise-wide cryptographic assessments to identify vulnerabilities and create tailored migration plans. Their phased implementation approach follows a proven "plan, build, run" framework that minimizes disruption while maximizing security posture.

Starting with cryptographic inventory and risk evaluation, Accenture guides clients through each stage of the journey, from initial proof-of-concept deployments for high-risk applications to enterprise-wide rollouts of post-quantum solutions across the security stack. The end result is a hybrid system where both classical and post-quantum algorithms coexist, ensuring security against both current and future quantum threats.

Partners in app modernization, security, and Zero Trust

The Cloudflare and Accenture partnership helps organizations reduce cyber risk, improve performance, and simplify operations for greater efficiency and lower TCO.

Clients can modernize applications on a global scale with the shortest time to value. Cloudflare's single, unified platform with robust network connectivity, support for multi-cloud environments, and full-stack security services from DDoS attack prevention to API security ensure every employee and customer experience is trusted and optimized. Modern apps delivered via Cloudflare's CDN can benefit from post-quantum security while maintaining performance.

Cloudflare and Accenture unlock rapid, incremental value by meeting clients on their Zero Trust journey. Using Cloudflare's composable, cloud-native network and secure access service edge (SASE) capabilities, organizations can seamlessly incorporate their infrastructure into a globally interconnected, rapidly expanding network that delivers comprehensive protection against both current and future quantum threats.