twimbit

The post-quantum imperative for financial institutions

Sponsored by f5

Post-Quantum Cryptography (PQC); foundational for future security

“Q-Day” is the moment when quantum computers achieve the power to break today’s encryption, a critical threshold signaling a new era in cybersecurity. As quantum technology rapidly progresses, this milestone highlights the urgent need to rethink how we protect sensitive information.

Post-quantum cryptography (PQC) refers to a new generation of cryptographic methods designed specifically to be secure against the potential threats posed by quantum computers.

“Harvest now, decrypt later” attacks are already underway. Adversaries can store encrypted data today and decrypt it later using quantum systems, compromising contracts, transactions, and sensitive records long after they are created.

In response, National Institute of Standards and Technology (NIST) in the US, has standardized quantum-safe algorithms designed to replace current cryptography vulnerable in a quantum-enabled world. Here are the finalized encryption standards:

#1

FIPS 203 –ML-KEM

Primary standard for general encryption

#2

FIPS 204 – ML-DSA

Primary standard for module-lattice-based digital signature

#3

FIPS 205 -SLH-DSA

For stateless hash-based digital signature

Potential impact on financial services organizations

#1

Data privacy concerns

#2

Loss of customer trust

#3

Slow end-customer adoption

Market adoption

Google’s Chrome 131, released in November 2024, supports hybrid post-quantum encryption to future-proof secure connections

In October 2024, Firefox started supporting quantum-safe encryption in secure website connections, and about 2% of a major CDN provider’s traffic now uses it.

In 2024, Apple upgraded iMessage with stronger, quantum-resistant encryption (called PQ3), designed to protect messages even from future quantum computers

Major tech players like Amazon and IBM and large banks are investing in post-quantum cryptography initiatives to secure their infrastructure before quantum computers arrive

Challenges for financial institutions

#1 Assessing legacy systems and cryptographic standards

#2 Strategic planning amidst uncertainty and the evolving quantum computing landscape

#3 Regulatory and compliance considerations

#4 Migration considerations such as, scale, backend preparation, performance and resource impact, interoperability and backward compatibility, code singling and firmware

Quick wins for financial institutions

#1 Shut down unused APIs and apps to reduce your exposed surface instantly.

#2 Baseline AI-driven components to catch risky behavior before it scales.

#2 Implement automated attack surface monitoring to catch changes in real time.

#4 Build a provable, quantum-ready security baseline that stands up to scrutiny.

Long-term strategy: Planning now for tomorrow

#1 Developing a comprehensive cryptographic transition strategy

#2 Collaboration with industry partners, regulators, and technology leaders

#3 Continuous monitoring of quantum computing developments and adjustments to strategy

Key takeaways

#1 Quantum computing threats necessitate immediate action

#2 Transitioning cryptographic methods is critical and urgent

#3 Proactive planning today ensures secured financial operations tomorrow

Learn about top PQC challenges and how F5 solutions can help here.

ABOUT F5

F5 is a multicloud application delivery and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure every app—on premises, in the cloud, or at the edge. F5 enables businesses to continuously stay ahead of threats while delivering exceptional, secure digital experiences for their customers.

For more information, go to f5.com

ABOUT TWIMBIT

Twimbit is a research and advisory firm driven by a singular mission: to empower businesses making a difference. We specialize in providing invaluable industry intelligence to executives and teams, acting as a catalyst for innovation and growth. Twimbit's proprietary research platform seeks to revolutionize the way enterprises consume insights, making it effortlessly enjoyable and accessible to all.

www.twimbit.com