QuSecure

Scalable security for the post-quantum banking enterprise

As we accelerate faster toward a cashless society, banking institutions face an increasing number of cyber-attacks due to interconnected attack surfaces, ransomware, and emerging technologies such as deepfakes and 5G.

A smooth path to organizational quantum resistance

Protect data in motion or at rest from quantum and other emerging cyber threats on any system, anywhere. QuSecure's comprehensive enterprise **Quantum Security Management Suite (QSMS)** allows you to orchestrate post-quantum secure communications end-to-end, on any device, using proprietary quantum and classical technologies.

Steal Now, Decrypt Later: Within 5 years, malicious actors will use quantum computers to decrypt data stolen today.

The Internet was established to communicate. Securing data – which must be protected for decades – was an afterthought.

Digital banking platforms and forward-thinking enterprises are starting to assess quantum computing threats in order to future-proof data assets and bolster consumer trust. QuSecure offers:

- ✓ **Quantum resilience without hardware dependence**: Software-based, self-authenticating solutions enable deployment across all nodes in the network or cloud.
- ✓ **Standardization**: QSMS is built to U.S. Military standards using National Institute of Standards and Technology (NIST)-approved post-quantum algorithms in combination with proprietary software-based quantum and classical technologies.
- ✓ **Flexible access**: The only quantum-resilient products that can be from the cloud, hybrid cloud or on-premises behind the firewall. Achieve self-aware, lightweight cryptographic protection of all legacy and new systems.
- ✓ **Speed**: Hyper-fast and secure post-quantum channel drives faster throughput than Transport Layer Security (TLS).
- ✓ **Maximum security**: Generate up to 60,000 randomized quantum keys per second with variable length to secure your enterprise networks with maximum post-quantum protection.

QuSecure's patented, QSMS software-only security architecture overlays your current infrastructure and protects your data in motion, in use, and at rest – on any system, anywhere – from existing and emerging cyber-threats.

POST-QUANTUM NETWORK

Protect data at rest, in use, or in transit – wherever it resides or travels on the network – with QuSecure's patent-pending Quantum Transport Layer Security (QTLS), an entirely software-based solution.

QUANTUM KEY MANAGEMENT

Access the strongest enterprise-wide encryption solution on the market today. QuSecure uses quantum random number generation (QRNG), which creates the most random security key available.

POST-QUANTUM DATA AT REST

Define and enforce how your data is protected, who may access specific data, and what format that data will take when access is granted. QuSecure's products are compatible with your existing systems and applications.

> "We estimate that a single quantum attack on one of the five largest financial institutions in the U.S. that disrupts their access to the Fedwire Funds Service payment system would cause a cascading financial failure costing anywhere from **$730 Billion to $1.95 Trillion."**
>
> - *Forbes*, May 2021

WWW.QUSECURE.COM
(650) 356-8001

ONE FRANKLIN PARKWAY, BUILDING 950, 1ST FLOOR
SAN MATEO, CA 94402