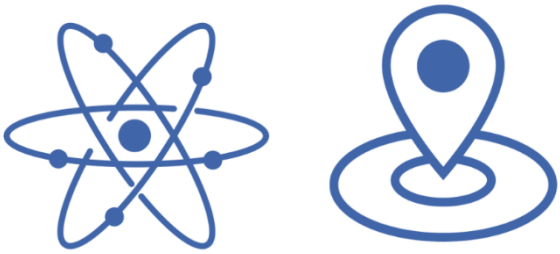
QuSecure

Scalable security for post-quantum space and satellite companies

As our dependence on satellites and other space-based assets continues to increase, so do attack vectors and security risks for these systems – many of which were developed before cybersecurity was a top priority. Service disruptions could cause substantial economic and intellectual property losses as well as create risk to our national defense systems. Quantum computers will be used to decrypt stolen satellite data and could be used to assume control of entire satellites.



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) orchestrates 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.

Forward-thinking space and satellite companies are starting to assess quantum computing threats to spacecraft, ground systems, and links between the two to safeguard the systems upon which our critical infrastructure relies. 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, 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.

WWW.QUSECURE.COM
(650) 356-8001

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

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.

"Take GPS, a technology whose precision is often taken for granted. All it takes is the production of a relatively inexpensive spoofer, and an attacker is able to command and control the uplink signal to a satellite... In the near-term, these kinds of attacks will likely remain posed by nation state actors but as more communications capabilities come online via space, the group of actors could expand to well-resourced non-state actors (e.g. criminal groups) seeking financial gain."

The Wilson Center, October 2020

WWW.QUSECURE.COM
(650) 356-8001

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