SPACE AND SATELLITE

Protecting your organization's future. Today.

QuSecure

READY FOR TODAY AND TOMORROW

CASE STUDY

Helping a Fortune 500 satellite company secure their digital assets

QuSecure was recently engaged by a Fortune 500 satellite company that handles highly sensitive data for its customers and provides in-flight connectivity to thousands of government and commercial aircraft.

Acutely aware of the SNDL threat of quantum computing, the company approached QuSecure to secure their digital communications and assets, and to ensure future protection against sensitive data breaches. Despite already offering best-in-class cybersecurity compared to their competitors, the company recognised the importance of upgrading their existing infrastructure to offer quantum resilience.

The challenge

Similarly to other satellite organizations, the company faced multiple challenges including:

- Orbit challenges associated with vulnerabilities with legacy encryption systems such as triple DES and key management
- Payload challenges associated with securing proprietary information between hosted payloads, trusted updates, compromised telemetry, tracking and control (TT&C) or compromised command and data handling (CDH) subsystems
- Ground station challenges associated with legacy IT and infrastructure management systems.

From QuSecure's perspective, key challenges included navigating the complexities of the satellite world, integrating seamlessly with the company's existing cybersecurity and legacy infrastructure, and providing a simple way to onboard their customers' fleets – ensuring all endpoints that sent or received data were achieved through a quantum resistant channel.

Another key challenge was that there were no cybersecurity standards and regulations set by a governing body.

Our QuProtect™ solution

QuProtect provided a solution for every endpoint and integration point, including satellite-to-satellite, satellite-to-ground, PEP accelerations, legacy assets and hybrid architectures. As part of our solution, we provided:

- A simple software upgrade, rather than a hardware solution, to ensure a rapid and seamless integration with legacy assets
- A secure protocol that was scalable across large space architectures and endpoints
- Variable trust capabilities, multi-path communications and reduced latency
- Base station and satellite capabilities which enabled encryption and decryption, encapsulate and decapsulate services, along with secure communications between the two
- Minimal risk by relying on proven, certified technologies, in line with the highest national standards
- Reliable and secure implementation, through microcode reference architecture which allowed for deployment on satellite and IoT devices alike.

Ready for today. And tomorrow.

The result was a rapidly implemented quantum-grade security solution that seamlessly integrated with the company's existing infrastructure – offering protection from the quantum threat today and in the future.

Key benefits of our solution

- Quantum Resilience
- Secured data in motion and at rest
- Cryptographic Agility
- Legacy integration
- Multi-Cloud and On-Prem Deployable

TEAM MEMBER SPOTLIGHT

Aaron D. Moore
VP Federal Ops, QuSecure

Aaron is a satellite and aerospace expert who formerly ran the largest dark sky facility for the federal government, and led teams at Lockheed Martin, Raytheon, and Northrup.

> *"Quantum computing threatens existing cryptographic systems promising to crack current encryption algorithms... Security and risk management leaders must assess enterprise dependence on cryptography and plan for agile migration to "postquantum".*
>
> **Gartner**

INTRODUCING QUPROTECT

Quantum-grade security.

For today's satellite organizations.

The quantum threat to satellite organizations is real, but preventable. Find out why you need to act today.

With the ability to simulate highly complex systems and interactions, the game-changing capabilities of quantum computers will provide an easy avenue for criminals and other adversaries to steal your data, exploit your organization and sabotage your operations.

Store Now, Decrypt Later (SNDL) is a common cyber attack where a bad actor will harvest an encrypted data source with the expectation of being able to decrypt it in the future. Once decrypted, it will be distributed or sold on the dark web, compromising the confidentiality and integrity of an organization's digital assets and information. For satellite organizations, the security risk is high – stolen satellite data could be used to assume control of entire satellites, while service disruptions could cause substantial economic and intellectual property losses, and create risk to our national defense systems.

In response, QuSecure has developed QuProtect™ – a robust all-in-one software-based quantum security solution that's quick to implement and effortless to manage. Highly compatible with today's technologies, and easily integrated across various devices, QuProtect offers a powerful and seamless solution for satellite organizations, so they are ready for today. And tomorrow.

QSMS Key Features

100% standards based & compliant
Including NIST & FedRAMP to provide trusted delivery of post-quantum resilience

Minimal to zero client-side installs required
Seamlessly upgrades managed and non-managed endpoints and devices, achieving BYOD encryption compliance

Easily integrated
Designed to be simple to deploy, operate and manage

Low-risk
Software-based solution optimized for the smallest changes with minimal disruption

Solves staged upgrade problems
Policy controlled backwards compatibility allows upgrades to be staged over time

Fully protects data
Delivers an end-to-end, zero trust oriented solution

Resilient to attack
Searches out and resolves attacks through deep instrumentation, ML-based threat and attack analytics, countermeasure deployment and remediation

Maximum Protection

- Strengthened encryption with a quantum entropy source
- Protects data at rest and in transit
- Built-in legacy support
- High availability and reliability with self-healing
- Active monitoring and remediation of threats
- Policy-based controls
- Zero trust architecture

Are you ready?
Contact us today

Set up a 15 min intro call

+1 (650) 356-8001
www.qusecure.com
info@qusecure.com