SPACE AND SATELLITE

Protecting your organization's future. Today.

READY FOR TODAY AND TOMORROW

QuSecure

CASE STUDY

Helping a Fortune 500 satellite company secure their digital assets

QuSecure was 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.

The Challenge & Opportunity

Aware of the SNDL threat and 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, the company recognized the importance of upgrading their existing infrastructure to offer quantum resilience.

In the space and satellite industry, a company faced a myriad of distinct challenges. They struggled with on-orbit challenges due to outdated encryption systems like triple DES and complex key management. Payload challenges arose from securing proprietary information amid hosted payloads, trusted updates, and potential compromises in telemetry, tracking and control, or command and data handling subsystems on a shared bus. Additionally, they dealt with ground station challenges linked to obsolete IT and infrastructure management systems.

> *"Bringing advanced security capabilities like QuSecure's quantum resistant crypto agility systems to orbit drives Accenture forward to better secure business on earth and throughout the space ecosystem."*
>
> **Tom Patterson**
> Managing Director, Emerging Technology Security, Accenture

Our QuProtect™ Solution

In response, we deployed QuProtect, a solution designed to navigate the intricacies of the satellite industry. Integral to QuProtect's success was its bent pipe configuration, enabling a seamless integration with the company's existing cybersecurity measures and legacy infrastructure.

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.

Integral to QuProtect's success was its bent pipe configuration, enabling a seamless integration with the company's existing cybersecurity measures and legacy infrastructure. This fundamental feature was pivotal in facilitating a smooth fleet onboarding process and establishing quantum-resistant channels for all data transmission endpoints.

In a field lacking established cybersecurity standards, QuProtect stands as a proactive, future-focused solution. It incorporates NIST Post-Quantum Cryptographic finalist algorithms and cryptographic agility, forming a resilient shield against quantum threats and positioning our client on the frontline of their industry's cybersecurity efforts.

QuProtect™ Key Solution Benefits

- ✓ Quantum safe connections to protect critical data with unchanged end user experience
- ✓ Gain control over your data with cryptographic agility
- ✓ Zero Trust Foundations
- ✓ Standards based & compliant
- ✓ Rapid, ready compatible deployment built to scale

SME SPOTLIGHT

Aaron Moore
Head of Engineering, QuSecure

Aaron is a satellite and aerospace expert who formerly ran the largest dark sky facility for the federal government. He served as a DARPA program manager for multiple restricted satellite programs, led the R&D for the virtualization of space platforms, and represented DARPA in OSD's Air Dominance Initiative on space-air layer integration tech. He has also led teams at Lockheed Martin, Raytheon, and Northrup Grumman.

> *"There are properties of space that we can exploit which allow us to have far greater security and agility when we encrypt data...space is not a luxury, it is a critical component of realizing the future of encryption."*
>
> **Lisa Hammitt**
> Chairwoman of the Board of Directors, Intelsat

INTRODUCING QUPROTECT

Quantum-grade security.
For today’s satellite organizations.

READY FOR TODAY, AND TOMORROW

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.

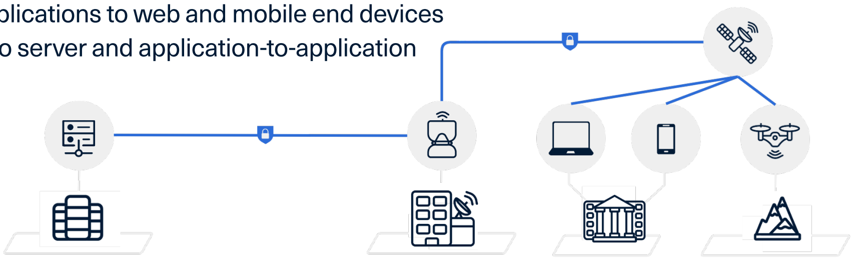
Store Now, Decrypt Later (SNDL) is a common cyber attack where a bad actor will harvest an encrypted data source with the expectation of being able to decrypt it in the future. Once decrypted, it will be distributed or sold on the dark web, compromising the confidentiality and integrity of an organization’s 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.

QuProtect™ Key Features

Quantum Safe Connections To Protect Critical Data With Unchanged End User Experience

- Web applications to web and mobile end devices
- Server to server and application-to-application



Cryptographic Agility

Full admin control over multiple post-quantum cryptographic algorithms, key lengths, and rotation frequencies that enable high entropy keys for post-quantum resilient connections.

Zero Trust Foundations

Enabling Zero Trust network architecture as defined by NIST SP 800-207

Standards Based & Compliant

Including NIST and compliance with the new Quantum Computing Cyber Security Preparedness Act for trusted delivery of quantum resilience.

A Scalable Solution – Start Today

Step 1. Initial Pilot Deployment In Hours

Quantum protect your most vulnerable network segment

QuProtect’s single day initial deployment does not require discovery nor a rip and replace overhaul to your mission critical systems. Select a small section of your network with critical data to protect with a low, fixed cost initial deployment on-prem or in the cloud.

Step 2. Prioritize & Plan

Expert guidance to plan your protection

QuSecure’s certified Solution Architects will work with you to design a prioritized plan to scale and protect the data and systems that matter most to you.

Step 3. Protection At Scale

Horizontally scale your quantum protection with ease

QuProtect’s cloud native architecture is built to scale with minimal effort to support larger enterprise PQC infrastructure needs.

Secure the future.
Today.

Schedule A Demo

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