FEDERAL OPERATIONS

Protecting our future.

Today.

QuSecure

READY FOR TODAY AND TOMORROW

CASE STUDY

Helping a Military Operations Center protect their critical assets

QuSecure

QuSecure was engaged by a Military Operations Center that handles a range of sensitive data from pattern of life data and information security infrastructure, to weapons control and logistics.

It was critical for this data to be protected immediately because a security breach would give an adversary the ability to access information in the theater, and sabotage the system and its operations. Acutely aware of the stealth infiltration and SNDL threat of quantum computing, the organization approached QuSecure to secure their data by protecting their cryptographic keys with PQC. They also wanted to ensure data integrity and non-repudiation (for data-at-rest protection) during the encryption, communication and decryption process.

The Challenge & Opportunity

The client came to us with a pressing requirement: the rapid delivery of post-quantum cryptographic keys to network terminus nodes, ensuring encrypted and secure communication between data feeds and warfighters at the edge. The urgency of the situation meant they needed a fast-to-deploy solution that could protect vital assets without impacting performance, throughput, or uptime.

Their challenges were manifold, including an expanding attack surface due to rapidly advancing adversaries, outdated security measures on legacy systems, managing a multitude of connected devices, and adherence to DOD and DNI requirements such as high bandwidth, low latency communications using existing equipment. Additionally, they needed to secure their command and data link transmissions.

At QuSecure, we understand that security is not just about protection, but also about efficiency and speed. QuProtect was deployed within hours, delivering post-quantum cryptographic keys to network terminus nodes at the edge, thus ensuring secure, swift data communication between data feeds and warfighters.

Our QuProtect™ Solution

Orchestrating Secure Comms
To begin, QuProtect's orchestration hub, Quark was deployed to enable enables high entropy key generation and key management services via an administrative dashboard.

Quark was deployed on-premise due to the sensitive nature of the data being protected.

> *"This is really awesome. [QuSecure] got set up and running in a couple of hours - and now we've got quantum keys in the US government."*
>
> **Dr. Dave Schuster** Chief Data Officer, NORAD & US North Command, United States Department of Defense, May 2022

Secure Comm Features
Once deployed, managed, quantum-resilient connections with cryptographic agility were enabled.

These connections were carried out via QuSecure's quantum-secure layer protocol that works in tandem with TLS.

The QuProtect solution enables Zero Trust network architecture as defined by NIST SP 800-207.

Ready for today. And tomorrow.

QuProtect seamlessly integrated with their existing systems, reinforcing security across legacy systems and various devices.

Furthermore, QuProtect met all DOD and DNI requirements, securing efficient cross-domain communication. By securing command and data link transmissions, QuProtect raised security standards, enhanced strategic capabilities, and offered a resilient shield against both classical and quantum threats, ultimately protecting the client's most sensitive data.

QuProtect™ Key Solution Benefits

- Quantum safe connections to protect critical data with unchanged end user experience
- Achieve mandated post-quantum compliance NSM 8 and 10 and H.R.735 memorandums.
- Gain control over your data with cryptographic agility
- Zero Trust Foundations
- Rapid, ready compatible deployment built to scale

SME SPOTLIGHT

Ret. Colonel Pete "Shadow" Ford
Head of Federal Operations, QuSecure

Pete has decades of experience from the Air Force cockpit to executive roles at Raytheon, Northrop Grumman and LLNL specializing in advanced aviation and space integration, communication protocols, WMD counterproliferation and advance threat developments.

SBIR Awards

QuSecure is a past recipient of SBIR Phase I, II, and III awards for post-quantum cryptography (PQC) Software as a Service. A SBIR Phase II to soon be awarded by the U.S. Army will provide cyber assurance enhancements for suitability on DoD networks and extend availability to Android devices. QuSecure remains Phase III eligible for Federal organizations requiring immediate compliance with PQC mandates.

INTRODUCING QUPROTECT

Quantum-grade security. For Federal Operations.

READY FOR TODAY AND TOMORROW

The quantum threat to Federal Operations is real, but preventable. 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 and exploit your organization.

Store Now, Decrypt Later (SNDL) is a common cyber attack where a bad actor 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 public sector, the security risk is high – stolen data has the potential to expose our nation's most sensitive secrets, bring global information systems to their knees, and destabilize the geopolitical balance of power.

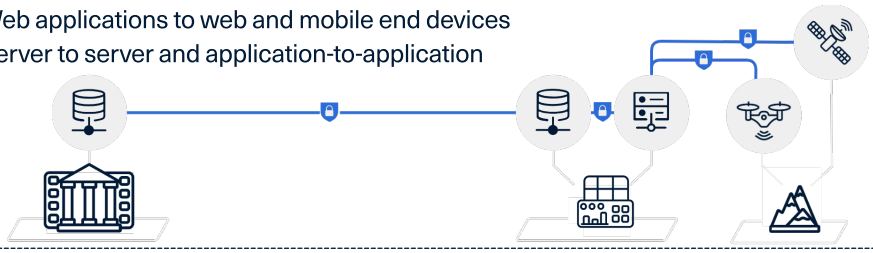
> *"Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC."*
>
> **Joseph R. Biden**
>
> President of the United States
>
> *NSM 10 Section 3, Paragraph 3*

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 is a powerful and seamless solution for Federal Operations, 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



Standards Based & Compliant

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

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

Easily Integrated With Legacy Systems

Designed to be simple to deploy, operate and manage.

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 Today

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