FEDERAL OPERATIONS

Protecting our future.

Today.

QuSecure

CASE STUDY

Helping a Military Operations Center protect their critical assets

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 and into the future 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

The challenge was to deliver post-quantum cryptographic keys to network terminus nodes, to encrypt and securely communicate data between existing data feeds and existing war fighters. Time was of the essence and the organization required a deployable solution to protect critical assets. It was also critical that performance, throughput and uptime was not impacted. Other key challenges to navigate included:

- Expanding attack surfaces – many systems were facing rapid adversary advances
- Legacy systems that were using outdated security
- A diverse array of connected devices
- DOD and DNI requirements such as high bandwidth, low latency communications across domains using existing equipment
- The need to secure command and data link transmissions

Our QuProtect™ solution

- An important part of our solution involved providing a QServer appliance for key generation and key management services to live on-site. Rather that accessing a QServer via the cloud, on-premise deployment was arranged due to the sensitive nature of the data being protected. The purpose of the QServer appliance was to:
- Provide a quantum key generation function
- Transfer post-quantum cryptographic keys to networked devices for the encryption and decryption process via QuSecure's quantum-secure layer protocol
- Manage keys for the decryption process
- Deploy policy to control and audit cryptography usage and upgrade
- Facilitate monitoring of the system functionality, to enable detection and remediation of attacks.

As a software-based solution, QuProtect enabled seamless upgrades of existing deployed platforms. Our solution was focused at a system level – addressing deployment issues, upgrade phasing, and cryptographic strength. We were able to address legacy system issues through protocol switching technology and provided monitoring to ensure all endpoints and channels for anomalous execution.

Ready for today. And tomorrow.

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

Key benefits of our solution

- Quantum resilience
- Session key frequency update driven by Quantum entropy
- On-premise secure deployment
- Crypto-agility
- Built-in moving target within session parameters
- Reference architecture microcode / lite footprint deployment

TEAM MEMBER SPOTLIGHT

Pete "Shadow" Ford
SVP 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.

> *"[By July 18th, 2022], agencies shall identify [non compliant systems] and a timeline to transition to compliant encryption, to include quantum resistant encryption."*
>
> **Joseph R. Biden**
> President of the United States

INTRODUCING QUPROTECT

Quantum-grade security.
For Federal Operations.

The quantum threat to Federal Operations 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 and exploit your organization.

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 Federal Operations, 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.

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 Federal Operations, 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