I. Company Overview

Founded in 2019, QuSecure is a post-quantum focused cybersecurity company that combines next-generation cybersecurity capabilities and the strongest encryption available into a comprehensive orchestration platform that is compatible with current network architectures and infrastructure. Our mission is to protect both government and commercial enterprise data against today's classical and tomorrow's emerging cyber threats simultaneously--across every network device and platform.

Based in San Mateo, California, QuSecure is a small business composed of ~60 employees distributed across the county. Our leaders have held C-Suite and Director level positions at organizations such as the National Security Agency (NSA), Google, Oracle, Raytheon, Northrop Grumman, USAF, and DARPA. We are a dual-use company targeting customers in the commercial and government sectors with a robust pipeline of partnerships and distribution channels.

II. Capability Statement

QuSecure orchestrates quantum-resistant cryptographic algorithms (under NIST purview) along with crypto agility to improve network security and resilience while enabling registered endpoints to remain functional in disconnected, denied, intermittent, limited bandwidth (DDIL) environments. Our solution, QuProtect TM, delivers a quantum-resistant, zero-trust framework that is compatible with existing infrastructure. It enables the Federal Government and the DoD to accelerate transition to quantum-resistant encryption while avoiding costs/time associated with exhaustive, time-consuming inventory of cryptographic systems and identification of encryption algorithms embedded in legacy code.

III. The Problem

Current security protocols and frameworks that use asymmetric and symmetric key encryption e.g., Transport Layer Security (TLS) and Public Key Infrastructure (PKI), to supply symmetric keys used in AES and SHA-256 encryption algorithms possess known cyber-attack vulnerabilities. Many experts project that advancements in quantum computing will enable adversaries to break the asymmetric cryptography used to transport and protect the key pair associated with TLS/PKI environments to ultimately compromise symmetric session keys. Though TLS can be modified to include post-quantum cryptographic (PQC) algorithms, implementation will be difficult and will not fully resolve the vulnerabilities inherent within the TLS protocol itself. We conclude that systems using current asymmetric cryptography techniques cannot fully satisfy Post-Quantum Cryptography (PQC) mandates and therefore require an alternate approach.

Additionally, cryptographic inventories are proving difficult/insufficient due to the inability to identify outdated and vulnerable cryptographic algorithms embedded in legacy code – a pre-existing condition that undermines the security environment needed for federal systems to operate in the post quantum era.

IV. QuSecure Solution

The QuProtect software platform introduces a secure and scalable process for the establishment of symmetric channel sessions with advanced crypto-agility features. The symmetric session keys are themselves encrypted using quantum-resistant algorithms and delivered via quantum-resilient channels established between the orchestration platform and endpoints. QuProtect uses a centralized orchestration platform to control symmetric session keys and quantum-resilient channels to endpoints/nodes for follow-on AES encryption of transported data.

QuProtect provides several modes of crypto agility that together improve network cyber-resiliency. The user interface (UI) allows operators to select and/or change (by individual node):

- encryption algorithm applied to the Quantum Secure Layer
- session key length,
- session key rotation rate,
- and multiple symmetric encryption algorithms (AES 256 variants),

in use at any given moment between orchestration platform and participating nodes.

In addition to current NIST-sanctioned encryption algorithms, QuProtect can easily accommodate any future encryption algorithm certified by NIST/NSA. It is also agnostic to the source of entropy used for symmetric key generation, i.e., Quantum Random Number Generator (QRNG) or NIST approved random bit generators. QuProtect is compatible with the majority of network infrastructure in use today enabling customers to migrate to PQC encryption without the requirement to rip and replace current infrastructure.

QuSecure has completed multiple beta demonstrations with commercial and government customers. We are currently performing on a Phase II SBIR awarded by Army ASA(ALT) in September 2023. This 18-month effort is focused on improving the performance and security of our software and production of a software development kit (SDK) that will extend QuProtect capability to the Android Tactical Awareness Kit (ATAK) and other Android devices. We were recently notified of tentative SIBR Phase I selection to investigate data transport security and integration requirements supporting USAF special missions.