QuSecure + Red Hat + immixGroup An Arrow Company

PUBLIC SECTOR

Quantum-resilient cyber security.

A QuSecure Post-Quantum Cyber Solution Powered By Red Hat

In partnership with Red Hat, QuSecure is launching the world's first post quantum cryptographic (PQC) security solution that enables government and enterprise businesses to address their post quantum cryptography business and technology challenges.

This introductory, Post Quantum Cyber solution branded QuProtect, enables organizations to integrate, deploy, and evaluate post quantum cryptographic solutions that suit their unique infrastructure environments.

Once integrated, the QuSecure cloud native, scale out architecture allows enterprises to scale out their baseline deployment as needed to support the larger PQC needs of their broader infrastructure environment.

The Problem

The impact of new technologies such as AI and quantum will accelerate cryptographic algorithm turn-over and requires businesses and government to dramatically reassess their data security postures. Foreign nation-states are spending billions of dollars to build quantum computers that can break current encryption methods that protect data today. This data is not only vulnerable to future attacks, but is compromised today via Store Now, Decrypt Later attacks.

Per Federal Mandates, Public Sector organizations need to:

- **Deploy cyber solutions that comply with NSM 8 and 10 and H.R.735 memorandums.**
- **Secure critical data and infrastructure against classical and quantum computing threats.**
- **Deploy legacy compatible, quantum resilient technologies that deliver infrastructure-wide security to ensure that quantum computers are not able to gain access to and decrypt critical data.**

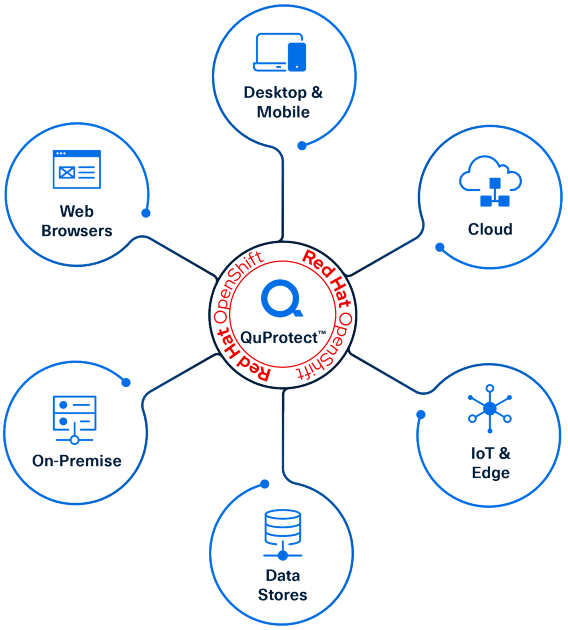
Post-Quantum Priority Focus Areas

FEDERAL OPERATIONS
JADC2, TRANSEC, Classified Data, NSS, Tactical Edge

CRITICAL INFRASTRUCTURE
Satellite-to-Satellite, Legacy Assets, Edge & IoT Sensors, Energy

Security Architecture

Our QuProtect software-based security architecture overlays your current infrastructure and protects your data in motion, in use, and at rest – on any system, anywhere – from existing and emerging cyber-threats.



Key Solution Benefits

Architectural Foundation Laid To Control, Protect & Enable Cyber Leaders For Today & Tomorrow's Threats

- Crypto-Agility
- Cryptographic Controls
- Zero Trust Foundations

Achieve Mandated Post-Quantum Compliance
Quickly address mandated post-quantum compliance without a heavy lift or shift of core infrastructure upgrades.

Controls & Actionable Insights For Peace of Mind
The QuProtect administrative dashboard enables new insights for network traffic along with audit capabilities, and cryptographic policy control.

Rapid, Ready Compatible Deployment & Built to Scale
Post-quantum protected data in transit via SaaS, without discovery and no rip-and-replace or disruption to mission critical systems. Initial deployment architecture is designed to scale as needed to support broader infrastructure.

Phase III SBIR
QuSecure is acquired under a Phase III SBIR making acquisition and deployment with the resulting compliance quick and easy. Enables fenderal funding through the Endless Frontiers Act.

INTRODUCING QUPROTECT™

Quantum-grade security.
For today's organizations.

QuSecure + Red Hat + immixGroup An Arrow Company

QuProtect™ A QuSecure + By Red Hat Solution 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.

Crypto-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

Low-Risk

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

Easily Integrated With Legacy Systems

Designed to be simple to deploy, operate and manage.

Easy Management & Control

The combined QuSecure Red Hat bundle enables easy management of the platforms full life-cycle of build and operation.

Flexible & Compatible

The underlying technologies enable easy plug and play usage and management consistently in different environments.

Strong Security Foundations Made Stronger

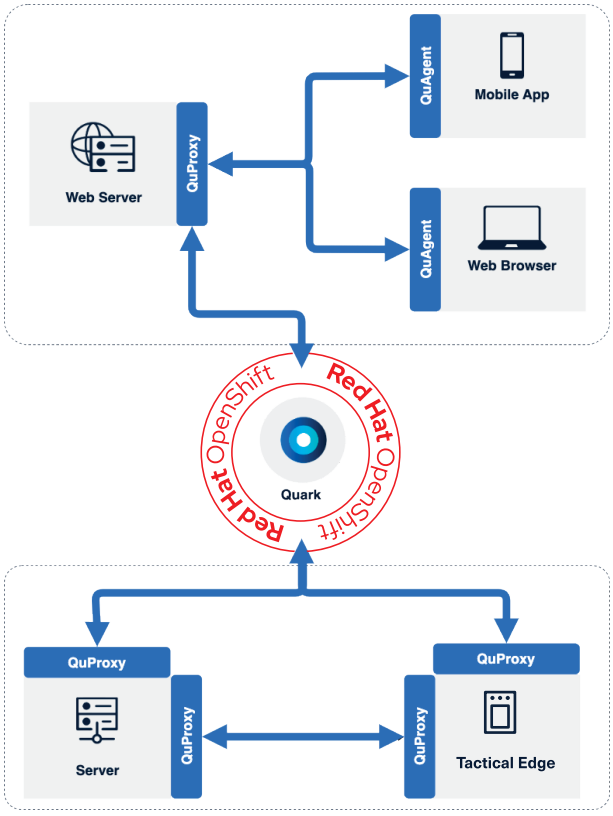
QuSecure extends Red Hat platform security into the quantum space. Default, out of the box, layered security combines with QuSecure's layered architecture to add quantum safe protection.

Minimal To Zero Client-Side Installs Required

Seamlessly upgrades managed and non-managed endpoints and devices, achieving BYOD encryption compliance.

QuProtect provides post-quantum resilience to all endpoints in a network. This robust all-in-one software-based quantum security solution is quick to implement and effortless to manage.

Secure Web Application Communication



Secure Application-to-Application Communication

Secure application-to-application communication capabilities are available for early access through our Diamond Partners

QuProtect™ Solves For These Top Risks

- Store Now, Decrypt Later attacks
- Asymmetric key exchange algorithms that need upgrading.
- Any pre-quantum device on the network representing an exploitable "weak link."
- Blindness into your cryptographic environment.

About QuSecure

Enterprise Cybersecurity SaaS that gives cybersecurity leaders the classical and quantum-resilient protection, assurance, and confidence they need so their organizations are ready for today. And tomorrow.

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