HYBRID CLOUD

Protecting your organization's future. Today.

READY FOR TODAY AND TOMORROW.

QuSecure

Hybrid cloud quantum-grade security.

With the ability to simulate highly complex systems, the game-changing capabilities of quantum computers will provide an avenue for criminals and other adversaries to carry out potentially catastrophic attacks on today's public key encryption. The hybrid cloud networks that are prevalent in today's digital ecosystems pose a unique need for quantum resilient security to extend to the cloud and beyond once data leaves the secure perimeter of an on-premise data center.

The Challenge

New & Advanced Attacks Enabled By Emerging Technologies

Quantum Computing promises to enable new and advanced cyber attacks. The most immediate threat is Store Now, Decrypt Later (SNDL) attacks, where data in transit it harvested for later decryption. If this data needs to be protected for several years (bank account information, PII, etc), it is imperative it has the proper quantum resilient encryption in place to protect it. When a cryptographically relevant quantum computer (CRQC) comes online, it can be used to break classical public key cryptography on a live communication sessions, as well as spoof public-key-enabled identities and certificates. Breaking communication sessions in such a way can allow bad actors taking control of transactions and sessions midstream.

Opportunity For Hybrid Cloud Environments

In an era where government and businesses both large and small rely on the cloud to augment their own infrastructure requirements, there is a growing need for control and visibility into network security.

The inherent flexibility of hybrid cloud environments introduce complexities in managing encryption in cybersecurity. The security and sovereignty of an enterprise requires the organization to constantly monitor and query the vulnerability of connections between its data center systems and cloud systems. Indeed, anytime data leaves the perimeter defenses of an on-premise data center to the cloud and beyond to a myriad of devices, networks and customer online applications, data and transaction sessions are at greater risk of becoming compromised. For these reasons, organizations need to be at the forefront of innovation to more completely control their end-to-end data transmissions.

Our Approach

QuProtect is 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, hybrid cloud environments, and easily integrated across multiple devices, QuProtect offers a powerful and seamless solution, so government and organizations are quantum ready today.

As the first and only US-founded, focused, and funded post-quantum security company QuSecure offers the world's first post quantum cryptographic (PQC) solution that enables orchestrated quantum-resilient end-to-end data in transit. Our holistic network solution empowers security leaders with post-quantum protection and controls over their cryptography.

Comprehensive Protection

- QuProtect enables PQC security from your datacenter directly through to every end user and their devices and back,
- On-premise systems are also protected directly to your cloud instance regardless of on-premise to cloud connectivity.

Cryptographic Controls & Monitoring

- Our control plane and administrative console enables administrators to verify that the PQC encryption is being properly utilized and immediately identify any exceptions.
- To enable the strongest data owner protection, QuSecure empowers security leaders to control the encryption and keys rather than being beholden to cloud providers.
- QuProtect enables real-time visibility of hybrid-cloud connectivity security.

Easy Integration

- QuProtect was built on trusted and verified components and can be integrated into your existing systems.
- QuProtect fits alongside critical business work streams running in the cloud or your data centers. It transparently adds capabilities like observability and security without requiring applications to undergo significant and costly upgrades.

In total, QuSecure provides a simple, efficient and effective PQC solution to the complexities and risks that hybrid cloud environments present organizations today. And tomorrow.

QuProtect™ Key Benefits

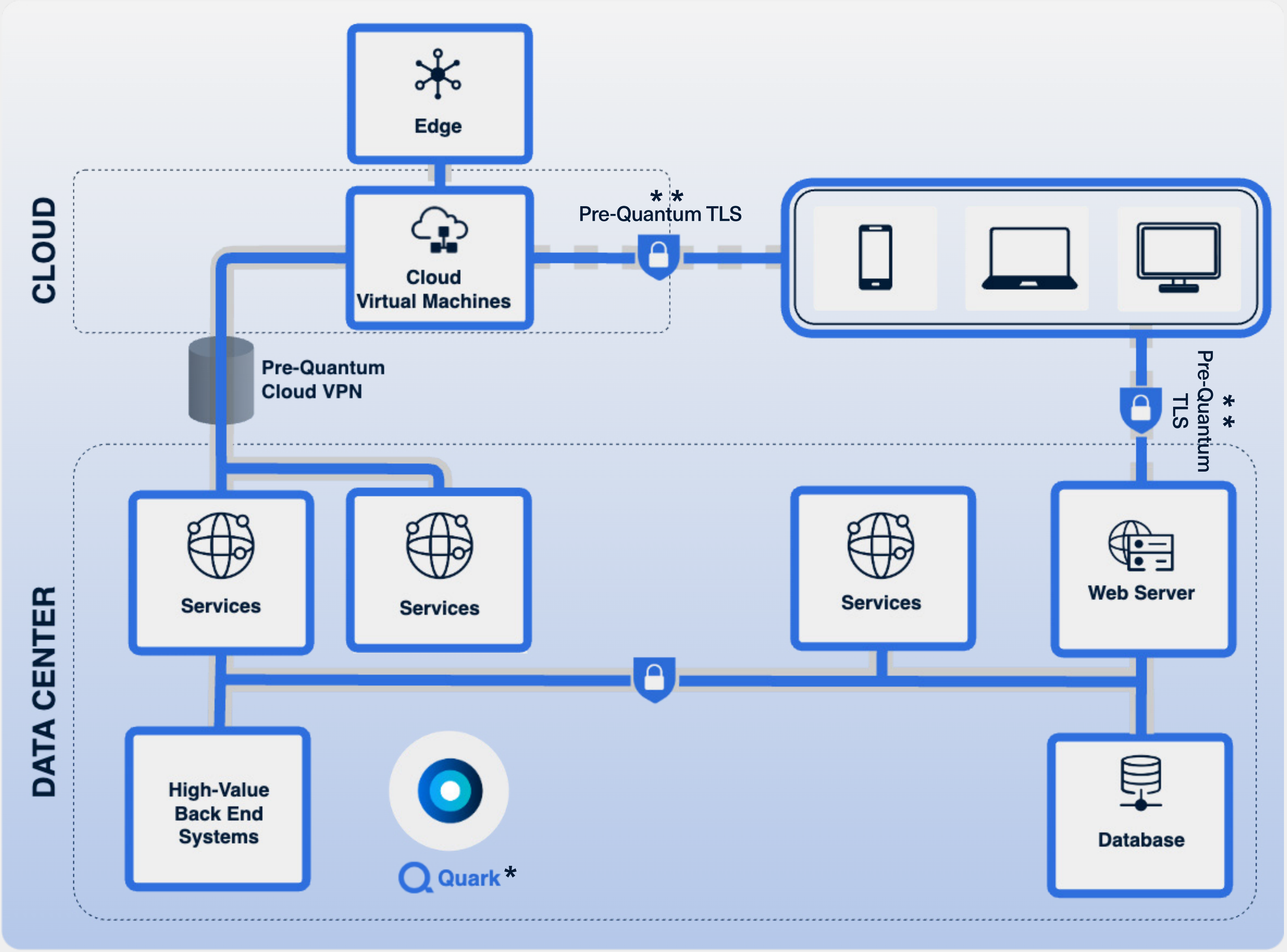
- ✓ Multi-Cloud and On-Prem Deployable
- ✓ Post-Quantum Data In Transit Protection
- ✓ Cryptographic Agility & Controls
- ✓ Direct Integration with Application and Device Support

TEAM MEMBER SPOTLIGHT

Kelly Collins
SVP of Customer Success

Kelly Collins has helped deliver advanced software solutions to global governments, financial institutions and enterprise customers for 40 years. Kelly was previously the Global Head of Cloud for SUSE where she managed the Hyperscaler organization working closely with AWS, Microsoft and Google. At IBM Kelly ran IBM's Federal Software Division and later the North American Cloud Engagement Hub responsible for working with IBM's most strategic clients journey to the cloud by optimizing high availability, containerization and cloud native modernization of key applications.

> *"As a trusted leader in the financial sector, we see it as an imperative to start now to protect our clients and assets from the quantum threat. It is critical to get this upgrade right, and we chose to work with QuSecure because their team and expertise is unparalleled, and they offer the only solution that makes the transition to post-quantum simple and robust for enterprise-scale networks."*
>
> **Cyber Security Leader**
> Fortune 500 Financial Services Firm



Our Solution

QuSecure was conceived to address and solve for both classical and post-quantum challenges simultaneously. The market for crypto-compromised devices running through hybrid cloud networks requiring upgrade from RSA and elliptical curve to post-quantum cryptography is enormous.

20+ billion network devices applications

7+ billion smart phones

QuSecure has envisioned a journey, a journey of safety for data and transactions. Thus, QuProtect was built to bring quantum resilience to every connection between every device and endpoint – to protect sensitive data wherever it travels. Where your encryption lives, QuProtect offers a post-quantum channel acting as a safe conduit for your data. Whether your data or transactions exist on prem or in the cloud, our software can handle endpoint as well as data center connections and cloud connections safely.

Rapid Deployment
Deployment can be as simple as a 2-hour process.

Compatible
QuProtect is fully compatible with existing systems and is designed to cause zero disruption.

Control
QuProtect enables you to own the entire connection path even in the foreign systems associated with hybrid cloud configurations.

Flexibility
Enable protection for inbound traffic, outbound traffic, or both connections per endpoint.

Scalable
As your organization grows, QuProtect's modular architecture is built for scale and easy integration with modern DevSecOps practices.

While the journey to cybersecurity is always ongoing, QuSecure is available to help make that trip easier, safer and more reliable.

🟦 Post-quantum channel protection.

* Quark orchestrates key delivery and protocols and can touch any endpoint in the network. Quark can be either hosted on-prem, or accessed via the cloud.

* * A hybrid layering of Post-Quantum and Pre-Quantum is the recommended NIST best practice for the time being to ensure a fall-back layer of protection. We can also deploy without TLS depending on customer preference.

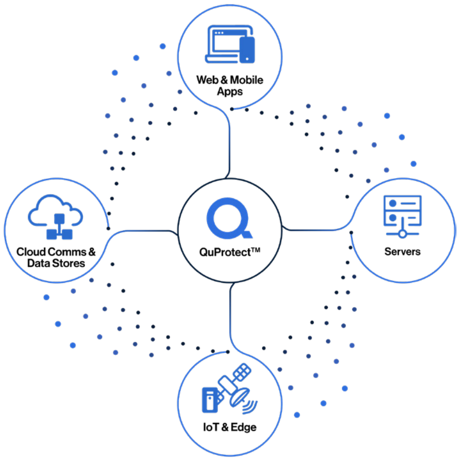
Quantum-grade security.
For today's organizations.

READY FOR TODAY, TOMORROW, AND TOMORROW

Our Vision For A Secure Future

Our charge is to bring post-quantum cybersecurity to government and enterprise to ensure a secure future.

We understand that the impact of emerging technologies including AI and quantum computing are already here and our specific cybersecurity solution, QuProtect, leverages today's technologies to bring post quantum protection to all end points in a network.



With QuProtect, your connections, from on the ground to cloud based facilities, will receive post-quantum protection. Additionally, your connections and transactions between services in the cloud will be protected affording you security from cloud providers. In total, QuSecure provides a simple, safe and effective post quantum cryptographic (PQC) solution to the complexities and risks that hybrid cloud environments present organizations 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.

Easily Integrating 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.

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 QuProtect Demo

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