HYBRID CLOUD

Protecting your organization's future. Today.

READY FOR TODAY. AND TOMORROW.

QuSecure

Hybrid Cloud Quantum-Grade Security.

The quantum threats to today's government and business organizations are real, but preventable. Find out why you need to act today.

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 datacenter.

The Challenge

Quantum Computing promises to enable new and advanced cyberattacks. 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.

In an era where companies 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 datacenter 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

In response to these challenges, QuSecure has developed QuProtect for Hybrid Cloud — 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 that that government and organizations are quantum ready today.

As the first and only US-founded, focused, and funded post-quantum security company with a software-based solution and pioneer in the PQC space, our QuProtect software orchestrates our solution to meet the needs of the end-to-end data in transit lifecycle. We are NOT an SDK solution but rather a holistic network solution that provides post-quantum crypto agility.

The end-to-end features of QuProtect allow for PQC security from your datacenter directly through to every end user and their devices and back . Additionally, your on-premise system is also protected directly to your cloud instance regardless of on-premise to cloud connectivity.

Our control plane allows you to verify that the PQC encryption is being properly utilized and immediately identify any exceptions.

QuProtect was built on trusted and verified components. The beauty of QuProtect the simplicity in which it can be integrated into your existing component to include Service Mesh and Kubernetes.

The key benefit achieved, when QuProtect is implemented, stems from the near-real-time visibility of hybrid-cloud connectivity security.

· Because QuProtect is effectively a drop-in, lightweight proxy, businesses will realize a multiplier effect on security while implementing a single solution.

These features fit alongside critical business workstreams running in the cloud or your datacenters. They can transparently add capabilities like observability and security without requiring applications to undergo major surgery and its associated costs.

To enable the strongest data owner protection, QuSecure allows YOU to control the encryption and keys rather than your cloud provider.

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.

Key benefits of our solution

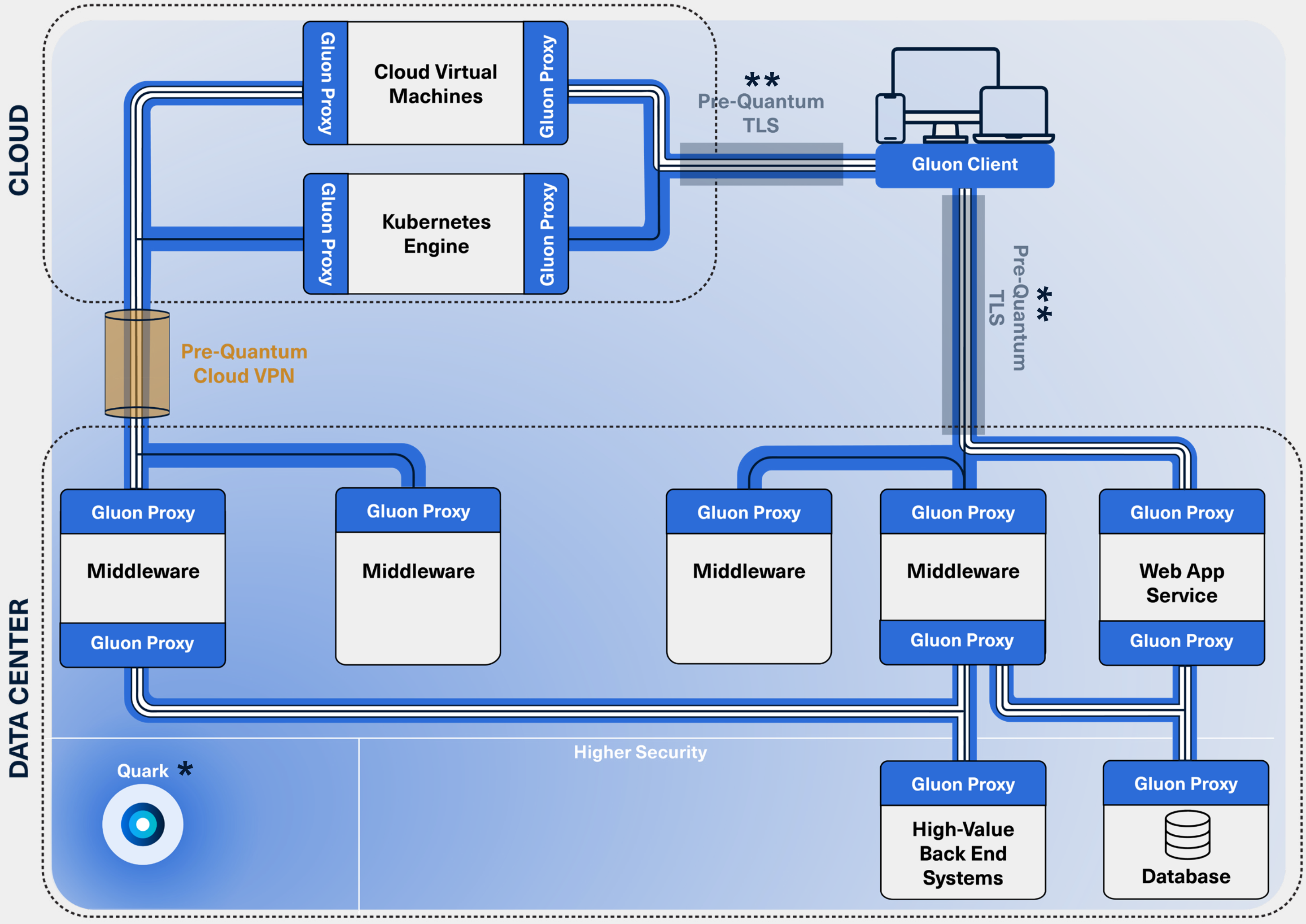
- ✓ Multi-Cloud and On-Prem Deployable
- ✓ Post-Quantum Data In Transit Protection
- ✓ Cryptographic Agility By Design
- ✓ Direct Integration with Application and Device Support

TEAM MEMBER SPOTLIGHT

Maralène Downs
Head of Compliance
QuSecure

Maralene previously led cloud risk at Bank of America, where she laid foundation for the public cloud risk framework, including a control framework and a governance body that decisions whether applications/services can be deployed to the public cloud. She began her career with 14 years as a research scientist at Bell Labs researching photonics and optical computing. Maralène holds a SB degree in Electrical Engineering and Computer Science from MIT as well as an MS in Electrical Engineering from Columbia University.

> *"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 / tunnel acting as a safe conduit for your data. Whether your data or transactions exist on the ground or in the cloud, our software can handle endpoint as well as datacenter connections and cloud connections safely. The features of QuProtect are outstanding but its real benefit lies in its simplicity. Deployment can be as simple as a 2-hour process. Additional simplicity exists in the fact QuProtect is fully compatible with existing systems and is designed to cause zero disruption. You are also in control as our solution enables you to own the entire connection path even in the foreign systems associated with hybrid cloud configurations. Additionally, our product is flexible. The Gluon Proxy provides you that flexibility as it enables protection for inbound traffic, outbound traffic, or both connections. Finally, 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.

▮|▮ Critical path for end-to-end post-quantum traffic.

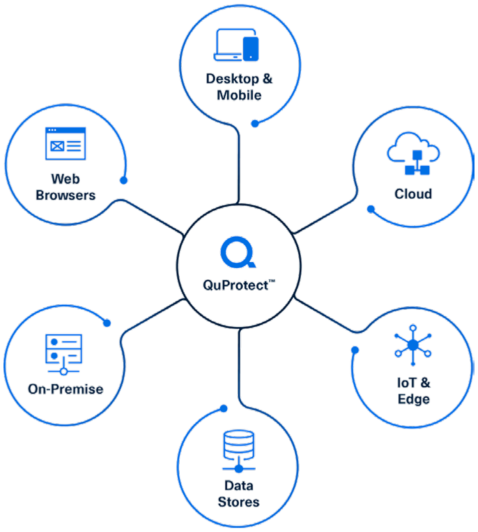
* Quark orchestrates key delivery and protocols and can touch any Gluon proxy in the network. It can be either hosted on prem, or accessed via the cloud.

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

Quantum-grade security.
For today's organizations.

READY FOR TODAY AND TOMORROW

QuSecure was created because its founders recognized, very early on, the benefits and more importantly the threats that come with quantum computing. Those threats are upon us today and are only growing in significance. For government and private business alike, the risks of inaction are not an option. 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 PQC solution to the complexities and risks that hybrid cloud environments present organizations today.
And tomorrow.



QuProtect for Hybrid Cloud Key Features

100% Standards-Based & Certified

Including NIST-approved-algorithms providing trusted delivery of quantum resilience. In progress for Fed Ramp and SOC certification.

End-To-End Data Protection

Supports Zero-Trust-Architecture, protecting the entire data lifecycle to deliver security at every endpoint, for data in transit from cloud, to server, to laptop, to edge and IOT.

Quantum-Resilient Key Strength

Entropy for cryptographic keys comes from a FIPS-certified Quantum Random Number Generator, mitigating the risk of using today's Pseudo-Random Number Generators.

Easy Client-Side Installs

Seamlessly enables upgrades for managed and non-managed endpoints and devices, achieving Bring Your Own Device encryption as well as end-user compliance.

Easily Integrated

Designed to be simple to deploy, operate and manage. Deployment solutions include hosted, on-premise, and cloud. Fully scalable solution to meet the demands of the largest organizations.

De-Risking The PQC Upgrade

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

High Availability

High Availability is designed in from the start, to ensure continuous service through all varieties of outages.

Solves Staged Upgrade Problems

Policy-controlled backward-compatible cryptography, allowing upgrades across your network to be staged over time. and cryptographic-agility delivers control of crypto-switching without service disruption.

Continually Monitored

Delivers visual insights and analytics, and compatible with active threat intelligence and monitoring platforms.

Contact us to help build out your solution.

Set up a 15 min intro call

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