

QUEVERYWHERE

Protecting your
organization's future.
Today.

QuSecure



Quantum-Grade Security.

Easy - Everywhere - All The Time.

We all take it for granted. Everyone expects it. Financial transactions and the movement of data appear seamless and near instantaneous for millions of people daily. Some call it the “Amazon effect” where everyone expects everything to be secure and delivered immediately. But how will this effect be impacted when your current encryption methods are at risk due to quantum computing?

As a CISO dealing in today’s world of speed, interconnectivity and high-volume transactions, you recognize how quantum computing will impact you and your areas of responsibility. Having to protect millions of end users who access your web browsers and applications is a daunting task. The idea of “embedded finance” is now ubiquitous with the integration of data and financial products into digital interfaces that individuals, companies, and governments rely on minute by minute. As McKinsey points out, the “possibilities are varied: customer loyalty apps, digital wallets, accounting software, and shopping-cart platforms, among others. For consumers and businesses using these interfaces, acquiring financial services becomes a natural extension of a non-financial experience such as shopping online, scheduling employees to work shifts, or managing inventory.” With the growing implications that quantum computing brings, our environment of multi-device, highly networked systems is at risk of decryption and thus collapse without a new form of protection.

The Challenge

The explosion of browser-based applications has been enormous over the last decade. Businesses, consumers and governments heavily rely on them to facilitate digital traffic, transmissions and transactions – and they are unbelievably vulnerable. Today’s CISO who deal in high volume

financial transactions, must feel like they are constantly trying to prevent water from leaking out of a colander. Data is everywhere and networks are porous. Our society runs on digital fuel:

Smart Phones
Desktop Computers
IoT Devices
Web browsers
Data Centers – Cloud & On Premise

These digital points of intersection where data and financial transactions connect leave us open to multiple entry points for cyber-attacks. In the world of encryption and public-key cryptography (PKC), you are only as strong as your weakest link. The ability for bad actors to penetrate any of these vulnerable points is numerous. With quantum computing, the security breakdown can come quickly and from nearly anywhere.

NEW THREAT INSIGHTS

Quantum Computing Promises To Enable New & Advanced Cyberattacks

Store Now, Decrypt Later

The most immediate threat is Store Now, Decrypt Later (SNDL) attacks, where data in transit (from any device or network) is 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.

Live Session Hacks & Spoofing

When a cryptographically relevant quantum computer (CRQC) comes online, it can be used to break classical PKC on live communication sessions, as well as spoof public-key-enabled identities and certificates. Breaking communication sessions in such a way can allow bad actors to take control of your transactions and sessions midstream.

QUEVERYWHERE IN ACTION

Web Browser Apps To Cloud Services & Data Centers

B2B2C



Bill wants to send \$50 to his friend Paige to pay her back for a dinner outing they had last week. When Bill uses his smart phone, he accesses his 1) mobile app or web browser to send that money into his mobile payment service, PayMo. The transaction starts its journey thru Bill's smart phone across 2) a very active network using public key encryption. From Bill's PayMo account, the funds sit at rest in the PayMo cloud environment until Paige, through her smart phone, wants to access the \$50. Paige moves those funds across 3) the same wide open internet environment to 4) her PayMo account. These touchpoints from device to app or web browser to cloud and data center, are all points of vulnerability.

QuSecure's software with QuEverywhere functionality provides a seamless zero-install solution that, when deployed on the browser or app, delivers PQC agility with end-to-end protection against classical and post-quantum attacks. Invisible and transparent to Bill and Paige, PayMo has protected the transactions, funds and data privacy in this example – clearly a competitive advantage in the financial marketplace that can be scaled in exponential fashion.



TEAM MEMBER SPOTLIGHT

Craig Debban
CISO, QuSecure

Chief Information Security Officer and former Global IT Director with proven ability to align technology strategy to business objectives while developing and managing high performing teams. Experienced in delivering large-scale enterprise solutions for Fortune 100 companies utilizing cloud based technologies and managed services.

CASE STUDY

In an era when companies large and small rely on widespread web protection, the need exists now to protect any website, application and device with post-quantum secured connections and sessions. The explosion of embedded finance includes retailers, business-software firms, online marketplaces, platforms, telecom companies, and original equipment manufacturers (OEMs). All these categories utilize browser-based, web enabled channels to conduct their business on a B2B, B2C and B2B2C basis.

“Among embedded-finance distributors and their end customers, demand is already maturing for a range of deposit, payment, issuing, and lending products (Exhibit 1). Risk is likely to remain a constraint on growth.”

McKinsey Oct 13, 2022
Embedded finance: Who will lead the next payments revolution?

That risk will increase exponentially as quantum computing enables decryption across devices, networks and systems. Despite these constraints, McKinsey estimates that products suitable for offering via embedded finance could account for as much as 50% of banking revenue pools. That number could increase significantly if post-quantum cryptography is implemented on all the points along the transaction path from consumer devices to commerce websites to payment facilities and banks.

Our Approach

With all that market opportunity potential in the making, the question remains as to how to tackle this risk and turn it into an advantage for your organization. Most financial institutions do not have the capabilities to build, sell, and service financial transactions and products in a quantum secure manner where current encryption is at high risk. CISOs will need to build a quantum resilient risk management framework that gives them confidence that the customers, clients and distributor partners they work with are acting within their risk appetite and in a compliant manner.

Demand for embedded finance is already growing in deposits, payments, issuing, and lending.

Embedded-finance distributors

Traditional retailers	Offer attractive financial products to enrich the customer checkout experience and incentivize brand loyalty and spending
Software firms	Strengthen the platform value proposition to drive merchant adoption, retention, and revenues
Marketplaces and platforms	Offer tailored financial products to improve the customer experience and increase merchant adoption, retention, and revenues
Telecom companies	Increase customer engagement and enhance the value of smartphone software and hardware with money-movement capabilities
OEMs	Simplify ownership and financing through subscription and other financing services

Embedded-finance products

Deposits	Transaction and deposit accounts that merchants and consumers can open and use from within an app or software platform
Payments	Money movement from within nonbank apps or software
Issuing	Prepaid, debit, and credit cards for customers and employees, issued from within business management software or apps
Lending	Unsecured lending embedded in business management software (eg, merchant cash advance) Secured lending for large purchases with underwriting and origination at point of sale

McKinsey Oct 13, 2022

Embedded finance: Who will lead the next payments revolution?



QuProtect

WITH QUEVERYWHERE FUNCTIONALITY

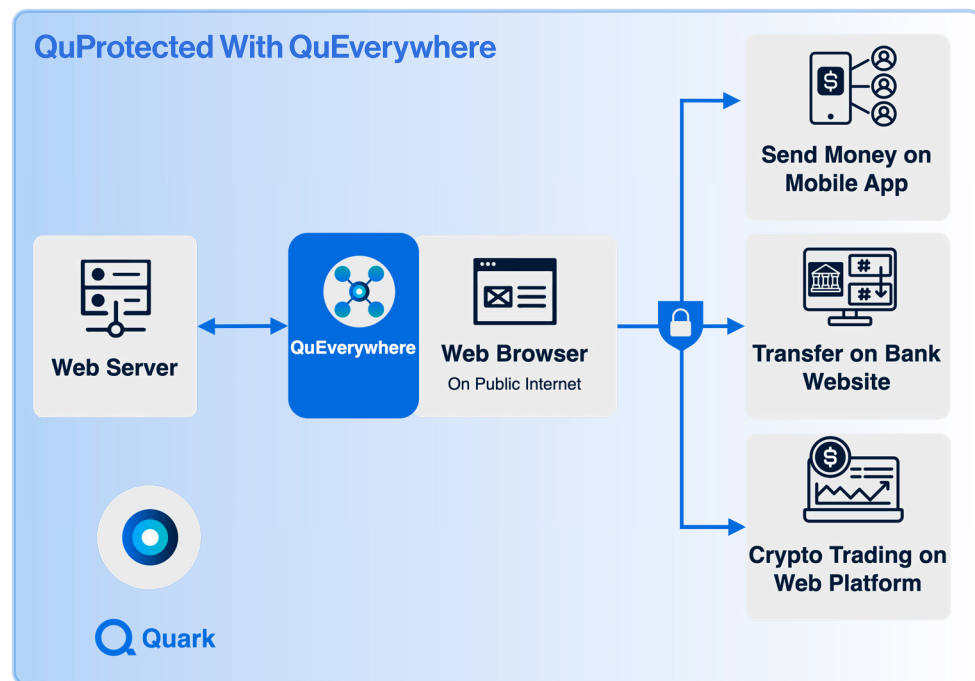
In response to these challenges and opportunities, QuSecure has developed **QuProtect with QuEverywhere functionality** — a robust all-in-one software-based quantum security solution that's quick to implement and effortless to manage. Highly compatible with today's technologies, QuEverywhere is easily integrated across multiple devices and offers a powerful and seamless solution, so that that government, businesses, 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 ability.

QuEverywhere Overview

- ✓ QuEverywhere is the end-to-end feature of QuProtect that allows for PQC security from your data center or cloud 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.

- ✓ QuEverywhere deploys to every end-user device whether mobile, desktop, or IoT, with zero-install for the end user and zero change in user experience. This ensures sessions where users view and provide sensitive data are post-quantum encrypted. The changes to the end-user will be invisible and seamless, but the benefits will be enormous.
- ✓ Our control plane allows you to verify that the PQC encryption is being utilized properly and immediately identify any exceptions.
- ✓ QuProtect was built on trusted and verified components. The beauty of QuProtect is in its simplicity because with zero-install it can be integrated into your existing component to include end-to-end Service Mesh and Kubernetes.
- ✓ The key benefit achieved, when QuProtect is implemented, stems from the near-real-time visibility of connectivity security in a multi-device and networked environment.
- ✓ These features fit alongside critical business workstreams running in the cloud or your data centers. 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 high volume transactional businesses face be it browser based, mobile device, IoT & Edge in cloud and data center environments. QuEverywhere helps to protect any device, anywhere, all the time. Today. And tomorrow.

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.

CRYPTO-COMPROMISED DEVICES

20+ BILLION
Network Devices Applications

7+ BILLION
Smart Phones

QuSecure has envisioned a journey – a journey of safety for data and transactions. Thus, QuProtect and its QuEverywhere functionality 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, on a mobile device, a desktop browser or a networked system, our software can handle endpoint as well as data center 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 – QuProtect is fully compatible with existing systems and is designed to cause zero disruption.

You are in control as our solution enables you to own the entire connection path even in the foreign systems associated with hybrid cloud configurations.

Our product is flexible. The Gluon Proxy provides you that flexibility.

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. The benefits of QuEverywhere can allow billions of devices, applications and networks to quickly and simply become quantum protected and thus QuSecured.

QUEVERYWHERE IN ACTION

Desktop Computers & Mobile Devices To Data Centers

B2C



Online banking apps are beginning to replace automated teller machines (ATMs). Paper checks are being replaced by electronic funds transfer (EFT). Today's digital natives are likely to have never stepped foot in a bank. The electronic transactions that consumers make with their banks take place over the internet and are open to a wide variety of vulnerabilities and attacks despite the public key encryption that purports to protect consumers. The following scenario bears this out.

The national bank, Bank On US, serves consumers across the country. A college student, Chris, attends school out of state and needs money for food and rent (among other collegiate necessities) from his parents. Both Chris and his parents have checking and savings accounts with Bank On US. Chris' parents go to their 1) desktop computer, hop on their browser to access their checking account. They transfer \$1,000 to 2) Chris' savings account at Bank On US. Chris then promptly transfers \$750 from his savings to 3) his checking account. These closed systems transactions are all within the Bank On US network but still susceptible to risk from bad actors across the internet. QuSecure's revolutionary software, QuProtect, has been designed to identify and safeguard from both

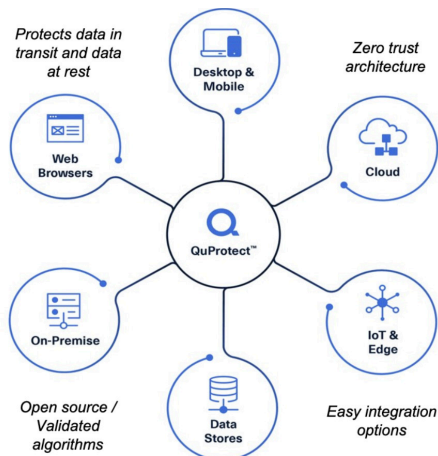
classical and post-quantum cyberattacks. It's QuEverywhere zero-install functionality is invisible and transparent to Bank On US customers yet still provides end-to-end PQC protection securing the privacy and security of customers like Chris and his parents making them QuSecured – confident in their bank and the safety of their funds.



Quantum-Grade Security.

For Today's Financial Organizations.

QuProtect with QuEverywhere 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, IoT and mobile device.

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.

"It is likely that a quantum computer will exist within the next decade that will be able to crack today's public key cryptography. [Everyone that relies] on public key cryptography will therefore need to transition to security protocols that quantum computers can't crack."

Morgan Stanley,
Oct 2020

QUEVERYWHERE IN ACTION

Browser Based Data In Transit To On-Premises Facilities

B2B



The concept of digital currency is now fact, not fiction. However, the growth and acceptance of crypto currency has presented new safety and privacy concerns.

Take the fictitious companies Coinbit and Zurianz. Zurianz wants to diversify a portion of its portfolio into crypto currency Coinbit to hedge against valuation swings. Zurianz accesses its Coinbit account via a desktop web browser to request a transfer to take a larger stake in Coinbit. As a closed system Coinbit must protect Zurianz's crypto currency transfer through the blockchain as the ledger is updated. However, bad actors today are stealing these blockchain records to decrypt in the very near future. With the rapid growth of quantum computing power thru individual quantum computers or linked networks of quantum computers, blockchain will be broken and Zurianz's Coinbit assets will be exposed and stolen.

QuProtect, with its revolutionary QuEverywhere functionality, protects the accounting movements from those thieves trying to use both classical and post-quantum decryption in this example. QuEverywhere prevents the breaking of the TLS session because the QuProtect software layers post-quantum encryption on top of TLS.

QuProtect is the leader in adaptive crypto to agility which, with its QuEverywhere functionality safeguards all the points of vulnerability in this case study. It is NOT an SDK solution but rather holistic network solution that provides financial institutions post-quantum crypto agility and protection.

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

