WEB APP SECURITY

Protecting your organization's future. Today.

QuSecure

CASE STUDY

QuProtect™ in action for financial transactions.

Secure web application communication.

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 today's current encryption standards that we rely on for secure data delivery in our web applications is not enough in the face of an evolving threat landscape.

As a business leader in today's world of speed, interconnectivity and high-volume transactions, the impact of quantum computing poses a risk today to your organization's and customer's critical data.

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 cybersecurity leaders 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 pre-quantum 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 emerging threats of quantum computing and AI, 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.

WEB APP SECURITY 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.

QuProtect's 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.

Widespread Web Protection For Embedded Finance

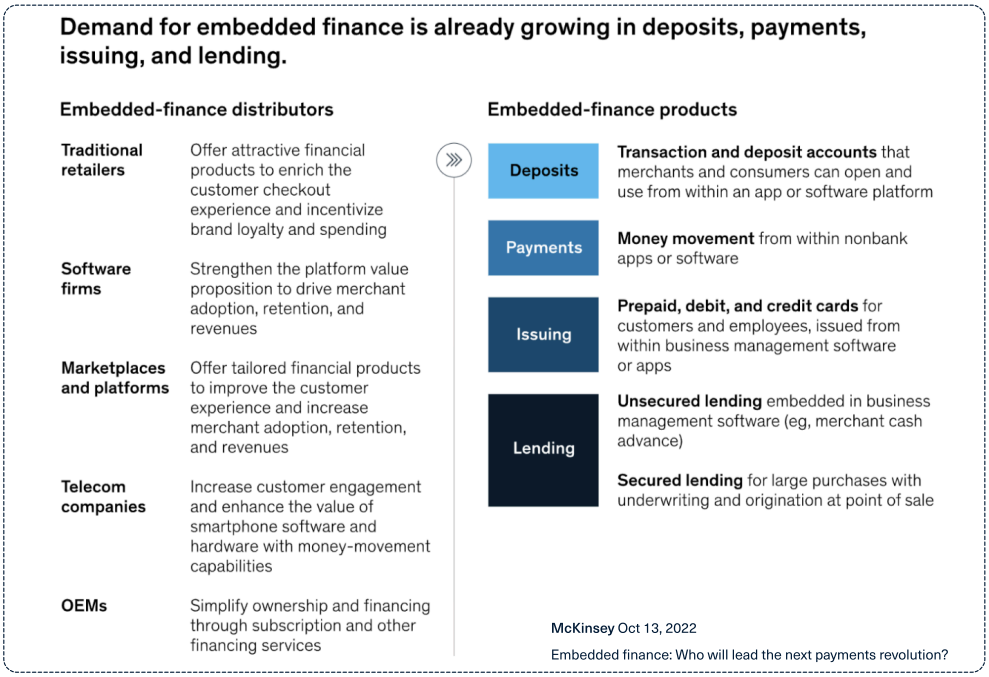
In an era when companies large and small rely on widespread web protection, the need exists now to protect any website, application and device with post-quantum secured connections and sessions. The explosion of embedded finance includes retailers, business-software firms, online marketplaces, platforms, 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?

As quantum computing enables decryption across devices, networks and systems the risk increases exponentially. 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 points along the transaction path from consumer devices to websites to payment facilities and banks.

The Opportunity

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. Forward looking cybersecurity leaders have an opportunity now 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.



About Us QuSecure

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 organizations to address their post quantum cryptography business and technology challenges and opportunities.

Our Solution

WITH WEB APP SECURITY FUNCTIONALITY

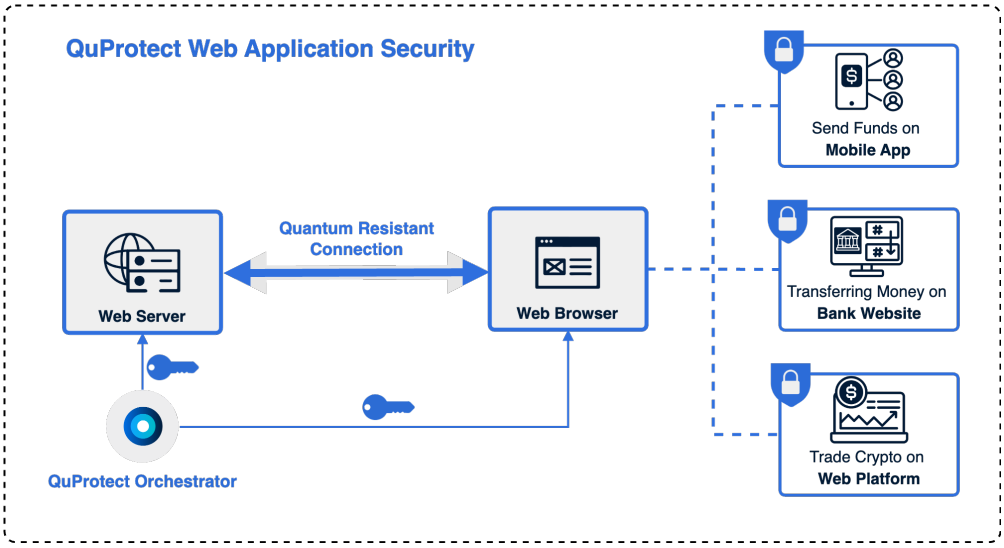
QuProtect
Our all-in-one software-based solution that secures critical data from classical and emerging AI and quantum threats anywhere it travels.

QuProtect with Web App Security Functionality
Protect communications between web servers and web applications on any device with ease. Deployed in under two hours, Web App Security provides quantum safe connections with no disruption to commsna and an unchanged end user experience.

Highly compatible with today's technologies, Web App Security is easily integrated with no disruption to comms.

Web App Security Overview

- Enables post-quantum, agile encryption for secure web application communication on any end-user device with zero-install or change in experience for the end user.
- QuProtect works in tandem with and provides advanced controls over today's encryption standard, TLS, as well as implementations of Hybrid Post-Quantum TLS.
- QuProtect's control plane allows administrators to monitor and manage secure connections.
- Administrators can easily select which NIST recommended post-quantum algorithms and TLS curves are utilized, and via cryptographic agility, easily adjust their selection in case of changing standards.
- QuProtect's cloud first architecture enables zero trust network architecture as defined by NIST SP 800-207.
- Through the administrative dashboard, QuProtect enables real time visibility of connectivity security in a multi-device and networked environment.
- QuProtect is easily and immediately deployed without rip and replace on both legacy and contemporary networks putting control and insights into your hands.



QuSecure provides a simple, efficient and effective quantum resilience 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. Web App Security helps to protect web communications. 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's 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 handles 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, modern and legacy, and is designed to cause zero disruption.

Control your cryptography and stay agile – Select NIST recommended post-quantum algorithms, manage key lengths, and key rotation with ease through the admistrative dashboard.

Ready today with no discovery required, QuProtect is built to scale enabling staged upgrades at your pace.

While the journey to cybersecurity is always ongoing, QuSecure is available to help make that trip easier, safer and more reliable. The benefits of Web App Security can allow billions of devices, applications and networks to quickly and simply become quantum protected and thus QuProtected.

> *"We chose to work with QuSecure, as they are the leader in intelligent switched crypto network security. Their team and expertise are exceptional, and they have made our transition to a quantumsafe environment simple and seamless."*
> **Sean Prescott, CTO, VeroWay**

WEB APP SECURITY 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 protects 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 suspectable to risk from bad actors across the internet.

QuProtect, is designed to identify and safeguard from both classical and post-quantum cyber-attacks. Its Web App Security 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 QuProtected – confident in their bank and the safety of their funds.

CASE STUDY

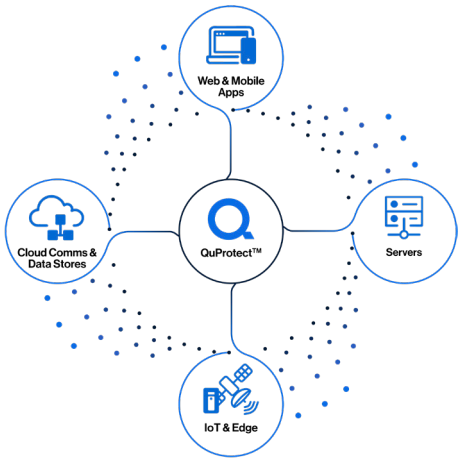
Quantum-Grade Security.
For Today's Financial Organizations.

READY FOR TODAY AND TOMORROW

QuProtect™ For Peace of Mind

QuProtect provides quantum-safe encryption to all communications in a network.

This robust, all-in-one software-based quantum security solution is quick to implement and effortless to manage.



- Protect all data in transit.
- Safeguard against Store Now, Decrypt Later attacks.
- Meet NSM 10 compliance

Key Features

Quantum Safe Connections To Protect Critical Data With Unchanged End User Experience

Web applications to web and mobile end devices.

Standards Based & Compliant

Including NIST and compliance with the new Quantum Computing Cyber Security Preparedness Act for trusted delivery of quantum resilience.

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. Rapidly change algorithms without disruption to communications or uptime.

Zero Trust Foundations

Enabling Zero Trust network architecture as defined by NIST SP 800-207

> *"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

WEB APP SECURITY 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 Web App Security functionality, protects the accounting movements from those thieves trying to use both classical and post-quantum decryption in this example. Web App Security prevents the breaking of the TLS and Hybrid PQ-TLS sessions by layering post quantum encryption on top. It further enables the customer to control whether to permit or mandate hybrid PQ-TLS sessions for their end users.

QuProtect is the leader in adaptive cryptography management and agility. It provides financial institutions the ability to leverage advanced security contols and protect against the quantum threat. The solution is also offered as an Android and iOS SDK.

Secure the future.
Today.

Schedule A Demo Today

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