DISA TECHNICAL EXCHANGE MEETING | DECEMBER 7, 2023

Quantum-resilient cybersecurity.
Delivered Simply

QuSecure

Agenda and Speakers

Agenda

Company Introduction
Threat Overview and DoD Need
Solution Overview
Live Demonstration
Past Performance
Q&A
Adjourn

Please use the chat feature to ask questions. We will do our best to answer questions as we receive them.

Additional Contact Information:
Pete Ford, SVP of Federal Operations | pete@qusecure.com
Herbert Race, Senior Program Manager | hrace@qusecure.com
Patrick Shore, Program Manager | pat@qusecure.com
Website:
www.qusecure.com

Aaron Moore

Head of Engineering
QuSecure
aaron@qusecure.com

Garrison Buss

Chief Strategy officer
QuSecure
garrison@qusecure.com

Company Intro

QuSecure orchestrates quantum-resistant cryptographic algorithms along with crypto agility to improve network security and resilience while enabling registered endpoints to remain functional in disconnected, denied, intermittent, limited bandwidth (DDIL) environments.

Company Snapshot

Year Founded
2019

Company HQ
San Mateo, CA

Employees
~60

Core Competencies

- Quantum-resistance
- Encryption
- Cryptography
- Cybersecurity

Additional Company Information

- **Clearances:** Multiple TS/SCI-eligible staff members
- **UEI:** WBKKDF2LAMV9
- **CAGE Code:** 8GGT0
- **Funding:** Series A
- **Staff Credentials:** Top Secret Clearance, CISSP, CRISC, PMO, PMP, CompTIA, CSM MPA, MBA, MS, JD, PhD degrees

Problem Statement

- Current security protocols and frameworks that use asymmetric and symmetric key encryption e.g., Transport Layer Security (TLS) and Public Key Infrastructure (PKI), to supply symmetric keys used in AES and SHA-256 encryption algorithms possess known cyber-attack vulnerabilities.
- Advancements in quantum computing will enable adversaries to break the asymmetric cryptography.
- Implementation of PQC algorithms will be difficult and will not fully resolve the vulnerabilities inherent within the TLS protocol itself.
- We conclude that systems using current asymmetric cryptography techniques cannot fully satisfy Post-Quantum Cryptography (PQC) mandates and therefore require an alternate approach.

Additionally, cryptographic inventories are proving difficult/insufficient due to the inability to identify outdated and vulnerable cryptographic algorithms embedded in legacy code – a pre-existing condition that undermines the security environment needed for federal systems to operate in the post quantum era.

Why Won't Existing Leaders Deliver A QuSecure Solution Or Better?

Network security is only as strong as its weakest point. In the classical computing era we could buy time by extending key lengths.

Cloud & OS Vendors

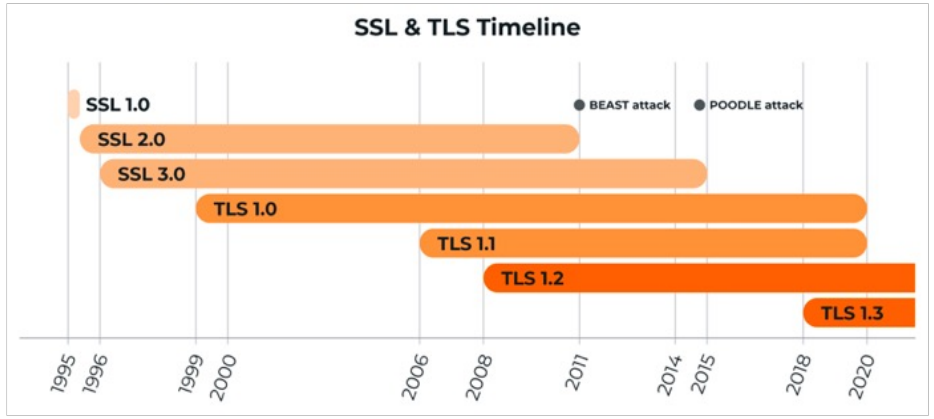
Not incentivized to build non-proprietary solutions or take approaches that aren't the minimum of what is in the standards.

- No incentive to be cloud and platform-agnostic (critical in today's environments)
- Upgrade cycles are slow, and vendors leave in old, vulnerable algorithms for backwards compatibility
- High security is difficult to implement as vendors optimize for mass-market high volume (low security)
- Competing business priorities means security is often a lower priority and will not receive funding or support

Platform Monitoring Vendors

Lack the expertise nor product footprint to deliver mission-mode cryptographic code required to enable control and monitoring of the cryptography (versus endpoint monitoring).

23 Years from SSL 1 to TLS 1.3



Networking Companies

Tools don't exist to audit cryptography.

- All encrypted data looks indistinguishable – it appears random

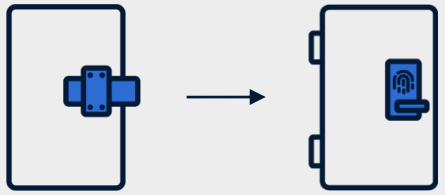
Successful penetrations into the cryptographic channel happen in between routing elements, where network vendors have limited visibility

Waiting on the IETF to publish a QRC protocol to replace TLS coupled with widespread adoption creates a high level of risk to network security.

The Quantum Threat event horizon is a rapidly approaching and will be catastrophic.

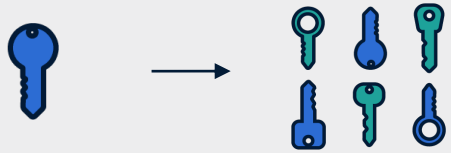
Ideal State Requirements

From Lack Of Visibility & Control - To Full



Entropy

High quality keys provide high entropy/randomness against quantum threats

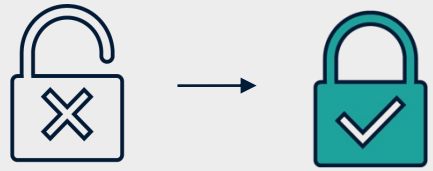


One Key vs. Multi Keys

Configure Frequency of Key Rotation for Forward Secrecy

Post-Quantum Cryptography

New NIST Standards Trump Classical Standards



Cryptographic Agility

Full Control of Crypto Algorithms & Key Lengths, Give Ability to "Hot Swap"

Works NOW On Existing Network Infrastructure
Enabling PQC version of Zero Trust Architecture

Ideal State Requirements Applied

The Quantum-Resilient Network Solution

SOLUTION APPROACH COMPARISONS

END-TO-END NETWORK SOLUTION

Provides a quantum-resilient encryption ability to all endpoints on your network.

Strong, Safe, Proven
Standards-based, certified encryption & keys enabling post-quantum communications channel.

Ready Deployment
Easy deployment of software-upgrade solution on all existing devices and applications.

Policy-Driven Cryptographic Agility
Enables phased, controlled upgrade across networks with backward compatibility.

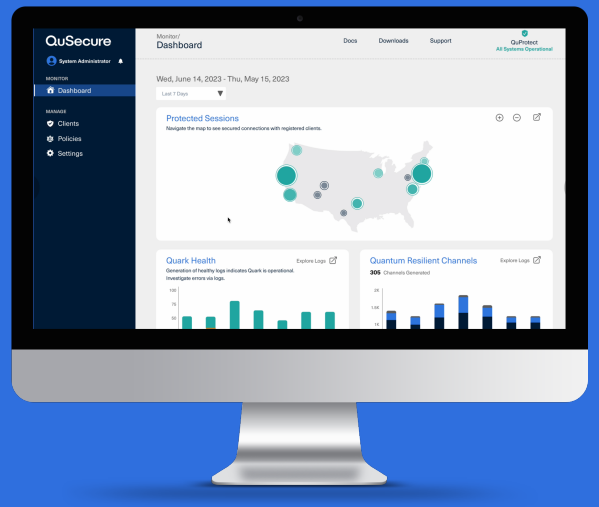
Zero Trust Architecture Foundations
Keeps Zero Trust network architecture IAW NIST SP 800-207

Attack Detection & Active Defense
Built securely is insufficient! – Our future means monitoring for attacks and actively defending.

QuProtect™

Quantum Safe Connections For All Your Critical Data; Cloud-native, on-prem and DDIL environments

QuProtect Orchestrator & Administrative Console



A central, post-quantum secure orchestration hub enables secure connections and control over those connections.

Secure Web Application Communications

Web Server — Web App on Any Device

Protection of 1,000 Registered Device Connections From End User's Browser And Mobile Devices To Customer's Web Server

Secure Application-To-Application Communications

Any Server — Any Server

Protection Of Data In Transit Between 5 Of The Customer's Application-To-Application Network Connections*

*Secure application-to-application communications are available for early access through our Diamond Partners.

Post-Quantum Hybrid Cloud

QuSecure has envisioned a journey of safety for data and transactions.
QuProtect is built to bring quantum resilience to every connection between every device and endpoint – to protect sensitive data wherever it travels.

QuProtect™

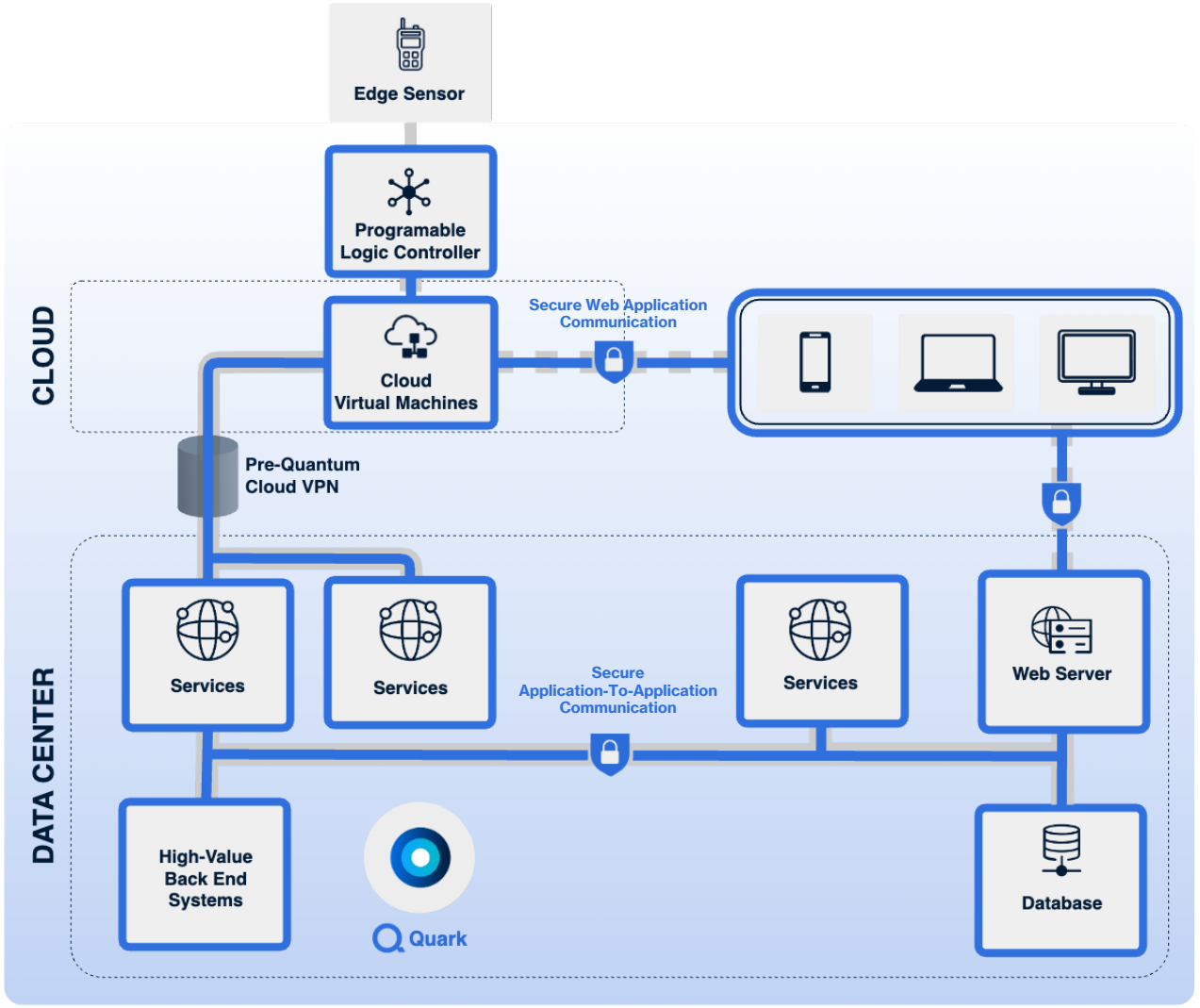
THE NETWORK OF THE FUTURE

MANAGEMENT CAPABILITIES & PROTOCOLS

Quantum Entropy	QKeys
Cryptographic Policy	Control
Post-Quantum Cryptographic-Agility	PQC

ACTIVE DEFENSE

Attack Monitoring and Adaptation	Insight
Zero Trust	Verify
Defensive Measures Deployment	Respond



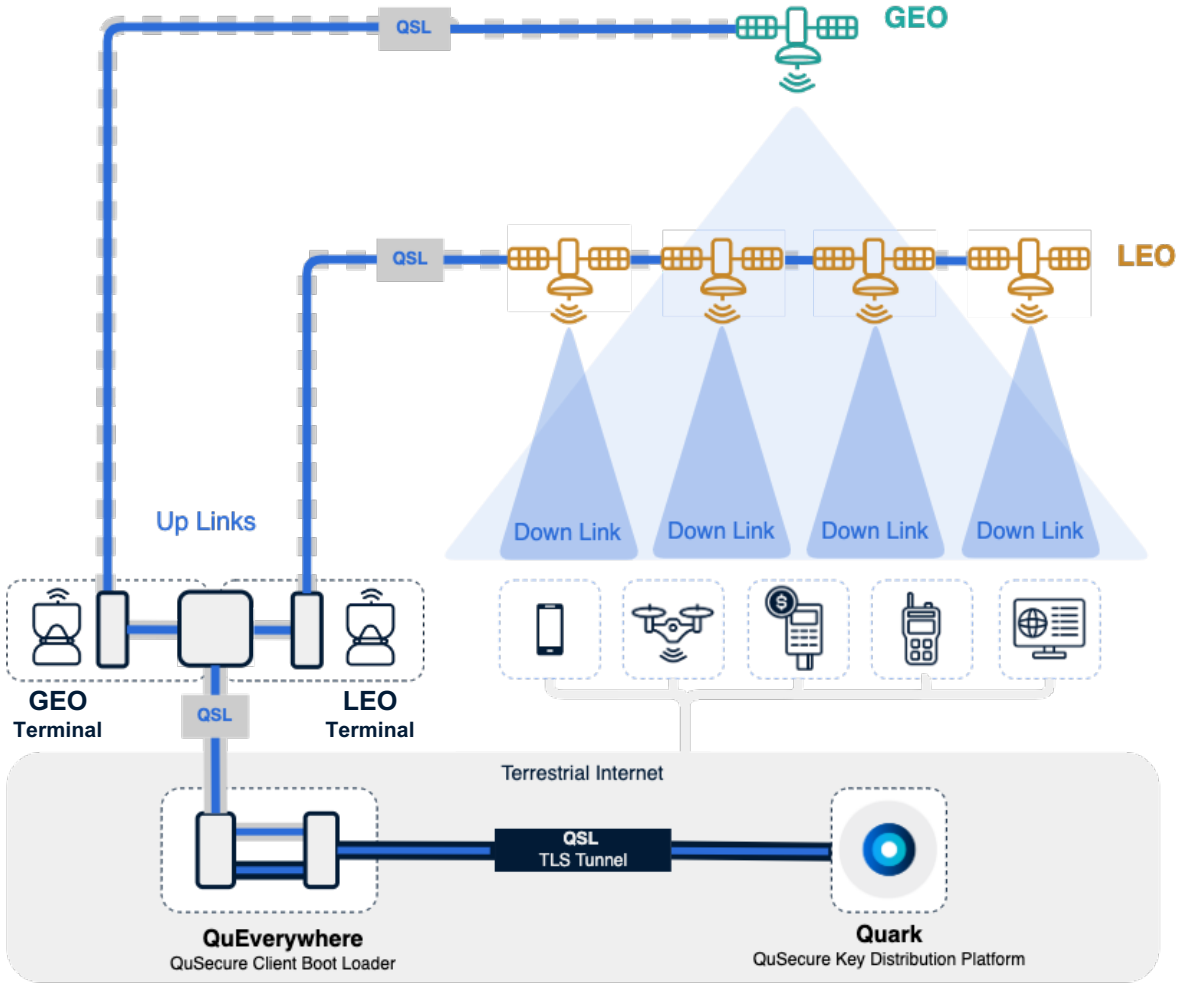
On Premise deployment illustrated above.
Cloud deployment available for Quark (the QuProtect orchestrator)

QuSecure

First Successful Multi-Orbit Communications Link Showcasing Post-Quantum Crypto Modernization

Post-quantum satellite communications enabled by QuProtect™

QuSecure encrypts TLS tunnel communication with quantum-resilient QSL with an SSL forwarded tunnel, which gets beamed to a Starlink satellite using a Starlink terminal for connecting devices in a secure fashion.



New Era in Quantum-Resiliency

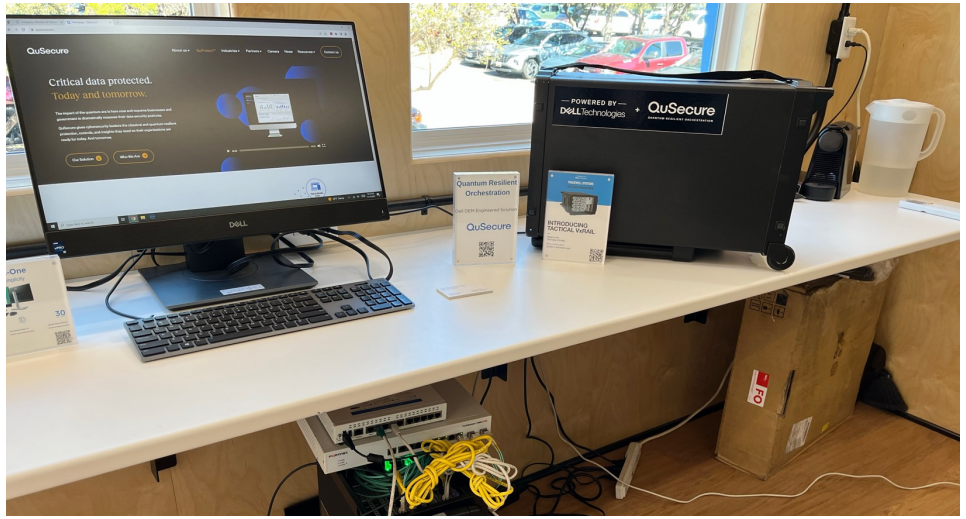
QuSecure and Accenture collaborate to secure space with post-quantum cryptography

>

QuSecure

Dell Demo at Alamo ACE

Dell Autonomous Mobile Unit



QuSecure *QuSecure Demonstration with Dell/Tracewell T-RX4000 (right)*

QuProtect Orchestrator (T-XR4000)

Live Demonstration

The Ecosystem of Post-Quantum Partners

"This is really awesome. QuSecure got set up and running in a couple of hours - and now we've got quantum keys in the US government."

DR. DAVE SCHUSTER - Chief Data Officer, NORAD & US North Command, United States Department of Defense

DELL Technologies

TRACEWELL SYSTEMS

TRUSTED INNOVATION

amazon

Red Hat

ARROW

accenture

CISCO

KLAS GOVERNMENT

Demonstration

Garrison Buss

QuSecure,
Chief Strategy Officer
garrison@qusecure.com

Past performance and accomplishments

Phase III SBIR, NORAD/NORTHCOM – Test of post-quantum CRYSTALS-Kyber KEM using real time ADSB data. This was the first every test of a NIST-candidate PQC Algorithm on real time data for the USG. See Fig.1

- Contact: Lt Col Ryan Corrigan, Ret. | rcorrigan@wzr-group.com
- Completed: June 30, 2022

Phase I SBIR, US Army ASA(ALT) – Feasibility Study related to the technical merit of the QuProtect, formerly QSMS, product.

- Contact: Robert Kimball | robert.m.kimball4.civ@army.mil
- Completed: March 15, 2023

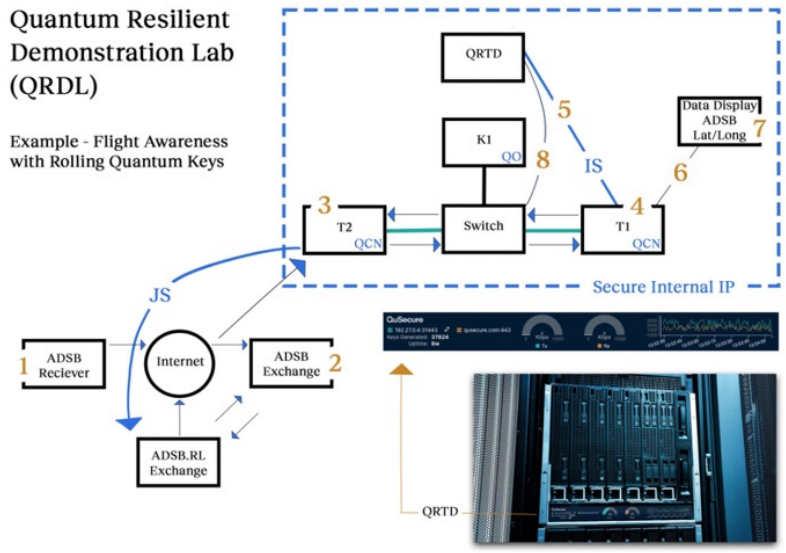
Phase II SBIR (In Progress), US Army ASA(ALT) – Hardening of core QuProtect components as well as development of an Android SDK.

- Contact: Robert Kimball | robert.m.kimball4.civ@army.mil
- PoP: 15 Sep 23 to 15 Mar 25 (18 months)

Phase I SBIR (In Negotiations) AFWERX – Feasibility Study related to demonstration of QuProtect for AFGSC.

AWS DDIL Experiment, AWS – Experimentation of the QuProtect product done in collaboration with AWS at the AWS DDIL lab in Arlington, VA.

- Contact: John “Hoss” DeRosa | johdero@amazon.com
- Completed: April13, 2023



1. Tracking aircraft mid-air thru ADSB Receiver
2. Information comes into open-source ADSB Exchange
3. Data captured querying in a controlled server T2 (to mitigate 3rd party outage risk)
4. Request from the T1 quantum connected node (QCN) over the quantum secure channel via the QuSecure environment and utilizing Kyber encryption. ADSB.RL passed through the quantum resilient channel (via quantum resilient channel switch) into the file store, all the while consuming keys from the Quantum orchestrator (QO) and Key Server (K1)
5. Quantum Real Time Display (QRTD) with perpetual feed connects data that moves throughout the protected QuSecure Internal IP environment between T1 and T2
6. The T1 user interface server can handle multiple user sessions
7. Data display indicates real-time ADSB latitude and longitude feed with speed and number of keys in utilization
8. Key consumption is related to byte count - the more bytes, the more keys generated

QuSecure Team Highlights

Your Guide

Dave Krauthamer

CEO

Founder and CEO Intelenex, 300 customers, sold to Oracle. 30+ years as a top CIO and information systems executive.

Aaron Moore

Head of Engineering

Former CTO Cyber Intelligence Northrup Grumman. CXO @ DARPA, NRO, IARPA, and NSA.

Rebecca Krauthamer

CPO (Chief Product)

Stanford University Symbolic Systems. Forbes *30 Under 30*, in Science. Top 12 Women in Quantum Computing. Quantum Futures Council – World Economic Forum. Former CEO Quantum Thought.

Skip Sanzeri

COO, CFO

Founder, COO, Author, *"Quantum Design Sprint"*.
5 company exits. 25+ years in C-level roles, M.P.A.CND, BA CMC.

Pete 'Shadow' Ford

Head of Federal Operations

USAF F-15 Fighter Pilot. Weapons School, Visiting Scientist/Professional at LLNL, Executive at Raytheon and Northrop Grumman.

Key Advisors

Lisa Hammitt

Board

Chairman of the board, Intelsat.

CTO & EVP Davidson Technologies. Former GVP Data & AI Visa.

Craig Hill

Board

Distinguished Architect, Cisco Systems, CTO Office

Ret. Rear Admiral Mike Brown

Former President of RSA. Director, Cybersecurity Coordination, DHS. Founder & President, Spinnaker Security.

Rene Haas

Current CEO, ARM

whose IP powers 95% of the world's smartphones. Non-Executive Director, Computacenter.

John Cosgriff

CEO of United Health One, United Health Group.

Louie Gasparini

Former CTO at RSA

Multi-time founder and storied cybersecurity professional

THANK YOU | Q&A

Help us secure the future. Today.

CONTACTS

Aaron Moore, Head of Engineering | aaron@qusecure.com
Garrison Buss, Chief Strategy Officer | garrison@qusecure.com
Pete Ford, SVP of Federal Operations | pete@qusecure.com

Additional Federal Operations Team Contact Information
Herbert Race, Senior Program Manager | hrace@qusecure.com
Patrick Shore, Program Manager | pat@qusecure.com

www.qusecure.com
info@qusecure.com

Address
1 Franklin Parkway
Bldg #930/1, Fintech Suite
San Mateo, CA, 94403

QuSecure