carahsoft® The Trusted Government IT Solutions Provider®

Quantum Buyer's Guide **for Government**

Discover solutions designed to help agencies achieve post-quantum cryptography compliance and safeguard sensitive data against future cyber threats.

FEATURING: ***Solution Areas • Success Stories Contract Vehicles • Vertical Policies • Upcoming Events*** carahsoft® The Trusted Government IT Solutions Provider®

Your Trusted Partner in Quantum Security Solutions

As quantum technologies evolve, so do the threats. A proactive quantum-readiness strategy is essential to safeguard sensitive data and ensure mission continuity. Carahsoft, The Trusted Government IT Solutions Provider®, supports the public sector in transitioning to post-quantum cryptography (PQC) with a robust portfolio of quantum solution providers to help agencies modernize encryption and meet emerging security requirements.

Transform Your Agency's Capabilities with Carahsoft's Quantum Portfolio:

- Shield classified and sensitive data from future threats
- Enhance operational speed and computational power
- Streamline mission-critical workflows
- Unlock advanced simulations with quantum-scale computing

Contact our industry experts today to empower your agency with the speed, security, and scale of quantum computing.

(844) 214-4790 | QuantumComputing@carahsoft.com | Carah.io/Quantum

Welcome to the Quantum Buyer’s Guide!

Table of Contents:

In government, innovation is often defined as leveraging advanced solutions to solve critical problems or meet emerging needs—whether for the broader community or within agencies themselves. Quantum Security aligns with this mission by addressing modern cybersecurity challenges with cutting-edge solutions that safeguard sensitive data and infrastructure.

As Federal Agencies work to meet mandates like National Security Memorandum 10 (NSM-10), which prioritizes quantum-resistant cryptography, and OMB Memorandum 23-02 (OMB 23-02), which calls for a transition to post-quantum cryptographic standards, innovations in cybersecurity are critical. These initiatives reflect a government-wide effort to prepare for quantum computing threats while ensuring long-term data protection and resilience.

Quantum Security’s solutions are designed to meet these urgent requirements, touching all aspects of operations—from IT infrastructure to data protection and digital transformation. Agencies such as the Department of Defense, National Security Agency, and Department of Energy are leading the way, and state and local governments are following suit by embracing quantum-safe technologies. Implementing these innovations requires strategic planning, forward-thinking leadership, and collaboration across sectors. In this guide, we share insights, case studies, and best practices for agencies striving to meet federal mandates, strengthen cybersecurity posture, and secure their operations against tomorrow's quantum-driven threats.

Troy Meraw
Program Manager for Quantum Solutions, Carahsoft

In collaboration with:

MARION SQUARE

Policies and Executive Orders

The U.S. Government is quickly ramping up its efforts to combat the risks posed by the advancements in Quantum Computers to its critical infrastructure. One key area of focus for Government agencies is encryption. As Quantum Computers continue to increase in capability and compute power, there is a very real risk of an adversary being able to break the current encryption standards by as early as 2030.

The World Economic Forum predicts that globally, over 20 billion digital devices will be impacted and need upgrade or replacement in the next two decades to remain safe from quantum cyberattacks (source in QED-C).

In response to this threat, the Trump Administration released the EO Sustaining Select Efforts to Strengthen the Nation's Cybersecurity in June 2025, prioritizing initiatives on quantum computing capable products.

NIST has been working closely with industry to identify and standardize quantum-resistant public-key cryptographic algorithms. This has been a multi-year evaluation program and NIST is expected to release its algorithm standards later this year.

NIST’s focus has been on providing Post Quantum Encryption standards for Public Key Cryptography specifically for:

- **Digital Signatures** - FIPS 204, Module-Lattice-Based Digital Signature Standard | CSRC (nist.gov) and FIPS 205, Stateless Hash-Based Digital Signature Standard | CSRC (nist.gov)

- **General Encryption** - FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard | CSRC (nist.gov)

In determining the timing of a move to Post Quantum Encryption, experts suggest Government agencies need to consider two key factors:

- **Migration time** - How long will it take to migrate the 100’s of thousands of applications, systems, etc. that will need to move to the new encryption standards?

- **Shelf life of data** - How long is the data stored in systems useful? The longer the shelf life, the greater the risk of “Harvest Now, Decrypt Later” when quantum computers are available.

With this as a backdrop, Carahsoft is working closely with our industry partners across the Post Quantum ecosystem to not only educate our Government clients, but also ensure that they have access to the right solutions to meet the Government mandated requirements and timelines for transitioning to Post Quantum Encryption.

Executive Order 14306

Executive Order 14306, published on June 6, 2025, amends Executive Order 13694 and 14144. It highlights the urgent need to prepare for cybersecurity risks posed by cryptanalytically relevant quantum computers (CRQCs), which could compromise current public-key encryption systems. The order reinforces the directives outlined in NSM-10 by requiring agencies to:

- Update NIST SP 800-53 by September 2, 2025
- Identify products that support post-quantum cryptography (PQC) by December 1, 2025
- Update the Secure Software Development Framework by December 1, 2025
- Ensure agencies transition to Transport Layer Security (TLS) 1.3 or higher by January 2, 2030, for systems under NSA and OMB oversight

NSM-10

Over the last few years, The White House, OMB and NIST have released clear guidance to agencies regarding the transition to Post Quantum Encryption (PQE).

The transition path started with the release of: NSM-10 National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | The White House. Which requires migration in National Security to Post Quantum Encryption by 2035.

M-23-02

OMB followed NSM-10 with a more detailed strategy, M-23-02 (whitehouse.gov), which states that agencies:

"inventory their active cryptographic systems, with a focus on High Value Assets (HVAs) and high impact systems. As used in this memorandum, the term "cryptographic system" means an active software or hardware implementation of one or more cryptographic algorithms that provide one or more of the following services: (1) creation and exchange of encryption keys; (2) encrypted connections; or (3) creation and validation of digital signatures."

M-23-02 further states:

The inventory must encompass each information system or asset that is any of the following, whether operated by the agency or on the agency's behalf:

- *A high impact information system;*
- *An agency HVA; or any other system that an agency determines is likely to be particularly vulnerable to CRQC-based attacks.*

Agencies should include information systems or assets that:

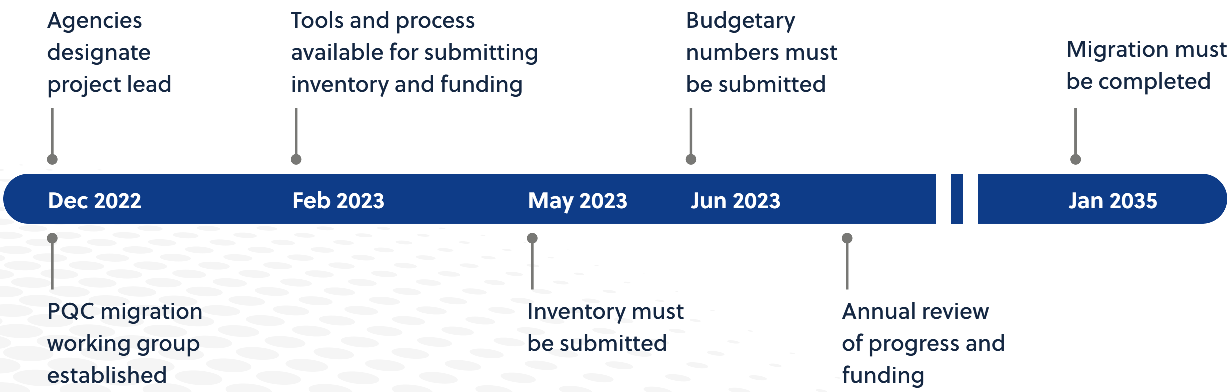
- *Contain data expected to remain mission-sensitive in 2035*
- *Are logical access control systems based in asymmetric encryption (such as Public Key Infrastructure)*

These inventories were to start in FY23 and continue annually until 2035. Along with providing cryptographic inventories agencies must also:

No later than 30 days after the submission of each annual inventory of cryptographic systems, agencies are required to submit to ONCD and OMB an assessment of the funding required to migrate information systems and assets inventoried under this memorandum to post-quantum cryptography during the following fiscal year.

The charts below outlines the annual requirements and timelines each agency must follow according to M-23-02:

Event/Activity	Actions following publication	Responsible Body
Designate cryptographic inventory and migration lead	Within 30 days	All agencies
Establish a mechanism to enable the exchange of PQC testing information and best practices	Within 60 days	NIST
Release instructions for the collection and transmission of inventory	Within 90 days	ONCD
Release instructions for funding assessments	Within 90 days	ONCD
Release strategy on automated tooling and support for the assessment of agency progress towards adoption of PQC	Within 1 year	CISA
Submit cryptographic system inventory	By May 4, 2023 and annually thereafter	All agencies
Submit funding assessments	30 days after submission of cryptographic system inventory, and annually thereafter	All agencies
Report testing of pre-standardized PQC	Ongoing	All agencies


Agencies designate project lead
Tools and process available for submitting inventory and funding
Budgetary numbers must be submitted
Migration must be completed
Dec 2022
Feb 2023
May 2023
Jun 2023
Jan 2035
PQC migration working group established
Inventory must be submitted
Annual review of progress and funding

Use Cases

Carahsoft and our vendor partners have solutions to address each step of an agency's Post Quantum Encryption migration path. From automated discovery and inventory to Post Quantum Encryption solutions that are compliant with NIST standards that address both general encryption and digital signature encryption requirements.

As quantum computers continue to advance, agencies must take appropriate countermeasures to protect sensitive data against cyber threats with cutting-edge encryption methods. To reduce current and future exposure to risk, the Public Sector requires organizations to safeguard high-value assets by implementing a comprehensive quantum-readiness strategy in preparation for the transition to post-quantum cryptography (PQC).

Carahsoft, The Trusted Government IT Solutions Provider®, supports Federal, State and Local agencies, as well as Healthcare organizations and Education institutions as they migrate to quantum-proof encryption algorithms. With an extensive portfolio of quantum solution providers, Carahsoft can help your agency identify and acquire the best-in-class software and services to achieve compliance with the Government's post-quantum cryptography initiative.

Carahsoft helps Government agencies accelerate mission-critical applications and security to stay ahead of the curve in this rapidly evolving field. Explore Carahsoft's innovative quantum solutions to learn how the Public Sector can leverage concurrent processing to:

- Protect classified data
- Improve operational efficiency
- Enhance computing capabilities

Quantum Security

Carahsoft's post-quantum cryptography solutions portfolio streamlines mission-critical workflows by performing advanced simulations and computations at an unprecedented scale and velocity.

Choose a technology vendor below to explore its Quantum Computing solutions and services.

ARQIT	CRYPTO4A	ENTRUST	Fortanix	GOLD COMET	GRAVEL ROAD GR
KEYFACTOR	PATERO	Qrypt	quantropi	Quantum Bridge	Quintessence Labs
QuSecure	SafeLogic Cryptography Simplified	SANDBOXAQ	THALES	TYCHON	walacor

Quantum Computing

Quantum computing leverages the principles of quantum mechanics to perform computations at speeds unimaginable with classic computers. From revolutionizing scientific research to optimizing complex business operations with quantum entropy, quantum computing holds the key to unlocking limitless possibilities for your agency in the digital landscape. Explore the portfolio below to access products and solutions that support your agency.

Explore the portfolio below to access products and solutions that support your agency.

aws	D-Wave	Microsoft	QUANTINUUM	vmware by Broadcom

Encryption Discovery & Inventory

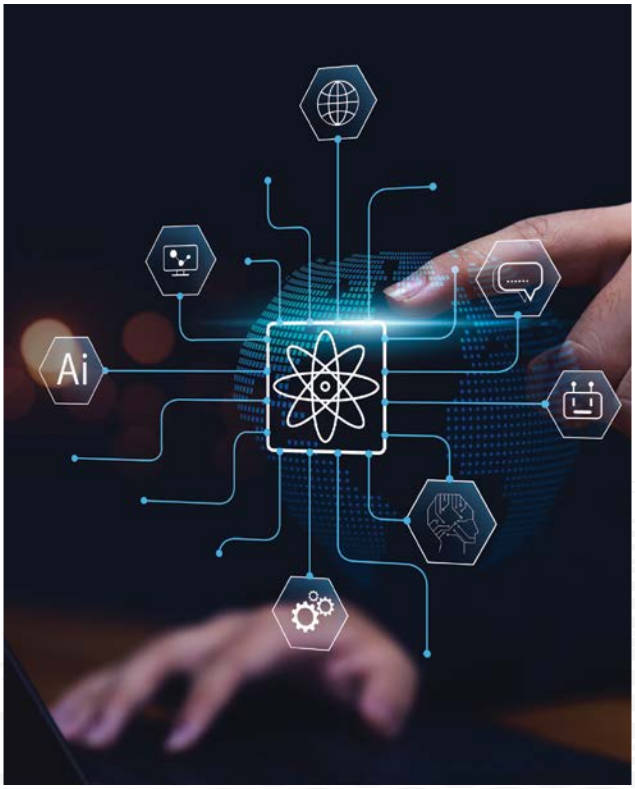
Carahsoft and our vendor partners have solutions to address each step of an agency's Post Quantum Encryption migration path. From automated discovery and inventory to Post Quantum Encryption solutions that are compliant with NIST standards that address both general encryption and digital signature encryption requirements.

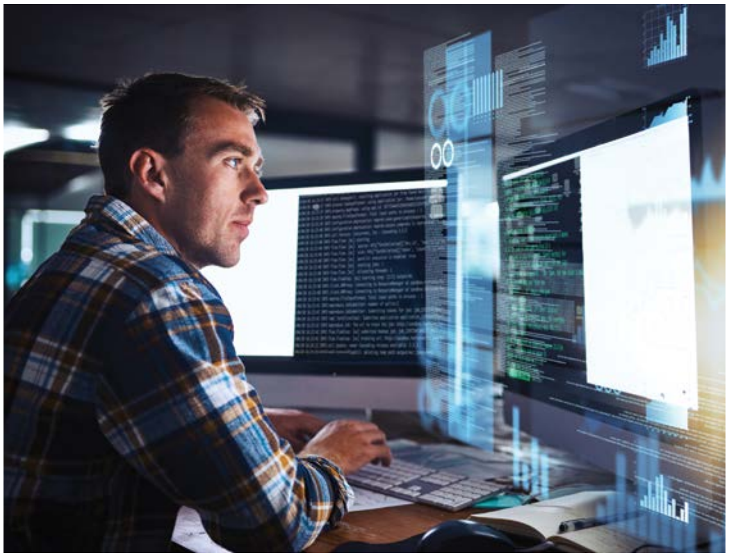
Per the requirements in M-23-02 each agency must on an annual basis *"inventory their active cryptographic systems, with a focus on High Value Assets (HVAs) and high impact systems."*

The discovery and inventory process includes looking at all deployed cryptographic systems used for creating and exchanging encryption keys, providing encrypted connections, or creating and validating digital signatures.

Choose a provider to learn more about their products and services.

KEYFACTOR | PATERO Quantum Secure Communications | SANDBOXAQ | TYCHON | ENTRUST





Post Quantum Encryption

According to NIST, the goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks.

NIST began a process to find and approve quantum-resistant encryption algorithms and has now released its Post-Quantum Encryption (PQE) standards:

- **Federal Information Processing Standard (FIPS) 203**, intended as the primary standard for general encryption. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation. The standard is based on the CRYSTALS-Kyber algorithm, which has been renamed ML-KEM, short for Module-Lattice-Based Key-Encapsulation Mechanism.
- **FIPS 204**, intended as the primary standard for protecting digital signatures. The standard uses the CRYSTALS-Dilithium algorithm, which has been renamed ML-DSA, short for Module-Lattice-Based Digital Signature Algorithm.
- **FIPS 205**, also designed for digital signatures. The standard employs the Sphincs+ algorithm, which has been renamed SLH-DSA, short for Stateless Hash-Based Digital Signature Algorithm. The standard is based on a different math approach than ML-DSA, and it is intended as a backup method in case ML-DSA proves vulnerable.

Carahsoft vendor partners can support both the General Encryption and Digital Signature requirements:

CRYPTO4A | Fortanix | QuSecure | quantropi | THALES

Quantum Secure Key Generation and Distribution

Quantum secure key generation is essential for federal agencies to protect sensitive data and communications against emerging quantum computing threats. As quantum computers advance, traditional cryptographic algorithms like RSA, ECC, and Diffie-Hellman, which rely on mathematical problems such as factorization and discrete logarithms, will be rendered insecure.

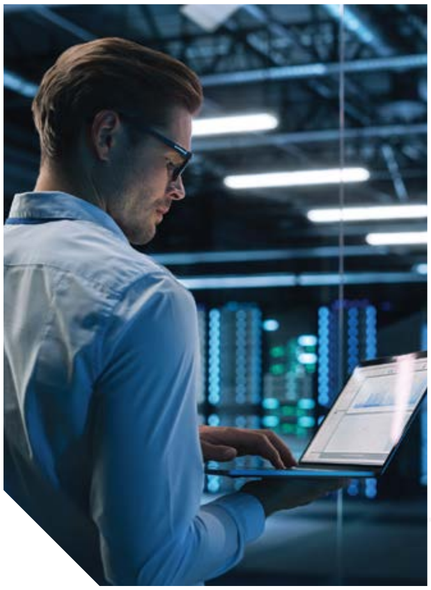
To address this, federal agencies must adopt quantum-resistant key generation methods that comply with federal mandates and ensure long-term security.

ARQIT | Qrypt | Quantum Bridge | THALES

Quantum key distribution (QKD) is a method of using quantum physics to create and distribute cryptographic keys that prevent data decryption. QKD is considered secure because the laws of physics make it impossible to clone or copy quantum states.

Choose a provider to learn more about their products and services.

Quintessence Labs | Qrypt



Entropy Solutions (Quantum Random Number Generators)

Quantum entropy is a way to use the randomness of quantum processes to create random numbers that are unpredictable and never repeat. These numbers can then be used to generate cryptographic keys, which are essential for secure encryption and communication.

Entropy is a fundamental part of encryption and cryptography, where it's used to measure the randomness of a key. The higher the entropy, the more random the data used to create a key, making it more difficult for hackers to break. Without a good source of entropy, cryptographic protocols can become vulnerable to attacks that exploit the predictability of the keys.

Quantum entropy can help address the vulnerability of traditional Pseudo Random Number Generators (PRNGs) to future quantum computers. Lower entropy makes it easier for a quantum computer to predict a key, so quantum entropy can help ensure that encryption remains secure.

Select a provider to learn more about their products and services.

QUANTINUUM | quantropi | Quintessence Labs | Qrypt

Hardware Security Modules

A Quantum Hardware Security Module (HSM) is an advanced security device designed to protect cryptographic keys and perform cryptographic operations in a manner that is resistant to quantum computing threats.

Choose a provider to learn more about their products and services.

CRYPTO4A | Fortanix | THALES

Success Stories

Many agencies are finding success by adopting quantum technologies to support their mission objectives. Discover how government customers are leveraging solutions from Carahsoft’s quantum technology partners to achieve their goals.

DISA & SandboxAQ – Quantum Resistant Cryptography (QRC)

The Defense Information Systems Agency (DISA) Emerging Technologies Directorate (EM2) has partnered with SandboxAQ to develop a Cryptography Discovery Service under the Quantum Resistant Cryptography Public Key Infrastructure OTA. This initiative directly addresses the "Harvest Now, Decrypt Later" threat, where adversaries steal encrypted data today with the intent to decrypt it once quantum computers become viable. Quantum-resistant cryptography (QRC) is critical for securing military operations, classified communications, and national infrastructure against these future threats. By integrating cryptographic agility, zero trust principles, and comprehensive encryption inventorying, the QRC Security Suite empowers DISA and DoD to identify vulnerabilities, monitor encryption use, and prioritize security measures against quantum-enabled cyber threats.

The Challenge:

While quantum computers capable of breaking encryption are still in development, data being stolen today could be decrypted in the near future—a threat known as "Harvest Now, Decrypt Later." Quantum-resistant cryptography or QRC, refers to cryptologic algorithms designed to withstand attacks from the classic computers of today, and quantum computers of tomorrow, which can break many of today’s encryption methods. QRC addresses this urgent problem by ensuring long-term protection of classified information and communications, securing military operations, and safeguarding critical systems against adversaries leveraging quantum capabilities. It's essential for maintaining trust and resilience in a post-quantum world.

The Solution:

Proper encryption, combined with strong key management and Zero Trust principles, can render stolen data less vulnerable to decryption, block unauthorized access, and detect anomalous activity to mitigate risks.

Inadequate cryptographic inventorying can leave defense entities vulnerable to data exfiltration, as exemplified by the following incidents:

1. **Iran-Affiliated Cyber Attacks on U.S. Infrastructure (2023-2024):** Iran-affiliated cyber actors gained access to and manipulated critical U.S. industrial control systems (ICS) in sectors including food and agriculture, healthcare, and water and wastewater.
2. **Impacket and Exfiltration Tool Attack on Defense Industrial Base (2022):** Advanced Persistent Threat (APT) actors employed tools like Impacket to exploit poor cryptographic practices within a Defense Industrial Base organization.
3. **Pro-Russia Hacktivist Compromises U.S. Water Systems (2024):** A pro-Russia hacktivist remotely manipulated control systems.

Key Takeaways:

- **Challenge:** Bad actors are stealing data in transit with the hope to be able to decrypt the data later with a quantum computer.
- **Solution:** Proper encryption, strong key management, and zero trust principles mitigate risks by protecting stolen data from decryption, blocking unauthorized access, and detecting anomalies.
- **Impact:** Stronger protection of your data in transit to prevent the worry of the “harvest now, decrypt later” threat.

SafeLogic
Cryptography Simplified

Kaseya Teams with SafeLogic to Strengthen Partner Security

Kaseya, a global leader in AI-powered cybersecurity and IT management, has partnered with SafeLogic to enhance encryption security across its products. This collaboration reinforces Kaseya's commitment to meeting FedRAMP standards by integrating FIPS 140-3 validated cryptographic solutions, ensuring stronger protection for sensitive data. By leveraging SafeLogic's expertise, Kaseya is upgrading its security framework to help customers stay ahead of evolving compliance requirements while safeguarding critical information.

The Challenge:

Organizations, especially those working with the U.S. government, must comply with evolving security regulations such as FedRAMP, FIPS 140-3, and NIST standards.

Keeping up with these stringent and frequently updated requirements is challenging, especially for IT teams managing multiple security tools.

The Solution:

Customers need a simple, effective, and future-proof way to manage encryption, maintain compliance, and protect sensitive data from cyber threats. Kaseya and SafeLogic provide a seamless solution by integrating FIPS 140-3 validated encryption into Kaseya's cybersecurity platform, helping organizations stay compliant, secure, and ahead of evolving threats.

Key Takeaways:

- **Challenge:** Staying on top of the latest security regulations that government agencies need to obey by (FedRAMP, FIPS 140-3, and NIST) that are evolving constantly.
- **Solution:** Integrated solution between Kaseya and SafeLogic giving government agencies a seamless solution with FIPS 140-3 validated cryptographic solutions into a single platform.
- **Impact:** Providing customers with enhanced encryption security, ensuring compliance, and keeping them protected against evolving threats.

walacor

Securing a Government Digital Twin with Walacor

A leading government agency responsible for intelligence and reconnaissance operations needed to secure digital twins used for maintenance and reliability predictions. Their goal was to ensure data integrity, prevent adversarial manipulation, and secure the digital twin against emerging quantum threats. With increasing concerns around AI poisoning and data tampering, the agency sought a solution that could lock down the integrity of the models created for their digital twin simulations. The government's technology lead was tasked with finding a resilient, scalable, and future-proof integrity solution that could be deployed without disrupting mission-critical operations.

The Challenge:

The agency's digital twin is a true-to-life digital replica of an aircraft created by completely scanning and modeling a real-world aircraft. However, they faced critical vulnerabilities:

- **Data Integrity Risks:** Potential adversarial data manipulation could corrupt the twin and create false results.
- **Quantum Threats:** Existing encryption techniques were vulnerable to quantum decryption.
- **Granular Security Gaps:** Traditional security models failed to enforce protection at the lowest data element level.

The Solution:

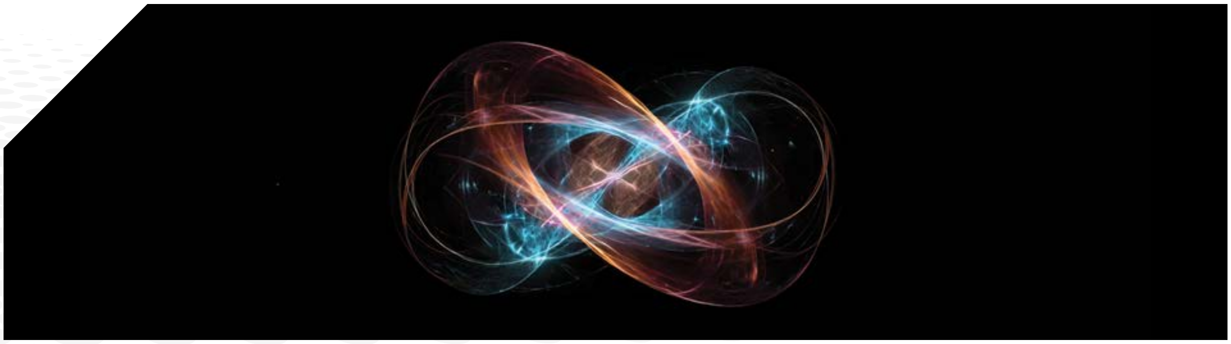
With direct support from Walacor's engineers, the agency's technology lead implemented Walacor's provable data integrity framework within an accelerated schedule. The rapid deployment was enabled by:

- **API-Based Integration:** Walacor's encryption and integrity solutions were easily embedded into the digital twin's existing architecture.
- **Zero-Trust Data Pipeline:** Ensuring immutable and tamper-proof workflow through secure data lineage tracking.
- **Automated Key Management:** Leveraging Walacor's derived encryption keys ensures the digital twin remained verifiable and encrypted.

Key Takeaways:

The deployment of Walacor's solution dramatically improved the integrity, repeatability and reliability of the agency's digital twin:

- **Guaranteed Data Integrity:** Ensured that incoming drone data was authentic, untampered, and trustworthy.
- **Quantum-Resilient Encryption:** Protected mission-critical intelligence from emerging quantum decryption capabilities.
- **End-to-End Visibility:** Provided complete data lineage from creation to consumption.
- **Compliance & Future-Proofing:** Aligned with government mandates for post-quantum cryptography.



SANDBOXAQ

HHS Leads the Way Towards Post-Quantum Cryptography

SandboxAQ was engaged by the U.S. Department of Health and Human Services (HHS) to develop the first post-quantum cryptographic inventory for a public health system, enabling the identification of cryptographic vulnerabilities and the creation of a remediation plan.

The Challenge:

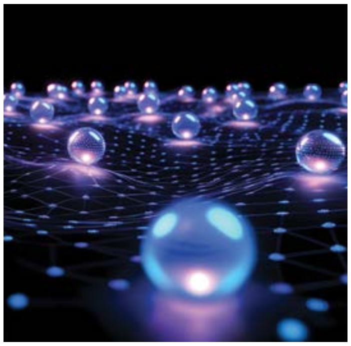
The U.S. Department of Health and Human Services (HHS) faced a limited timeframe to complete its cryptographic inventory before the OMB deadline. SandboxAQ successfully delivered a comprehensive inventory of the network and file system, identifying cryptographic vulnerabilities and noncompliant protocols, including FIPS 140-2, PCI DSS, HIPAA Security Rule, and HHS 405(d). This project was completed three months ahead of the OMB's deadline for the Post-Quantum Cryptography (PQC) inventory, ensuring HHS remained proactive in its security and compliance efforts.

The Solution:

SandboxAQ deployed AQtiveGuard, an end-to-end cryptographic management platform, to Cart.com's systems to help ensure compliance with new regulations. In only one week of scanning, AQtiveGuard identified vulnerabilities in a third-party vendor and an open-source library. AQtiveGuard recommended remediation actions that enabled the third-party vendor to upgrade its cryptography to approved cybersecurity standards.

Key Takeaways:

- **Challenge:** Getting the full PQC inventory of HHS network and file systems before the OMBs deadline and putting together a remediation plan for found vulnerabilities.
- **Solution:** SandboxAQ deployed their solution, AQtiveGuard, to help HHS perform the post-quantum cryptographic inventory that needed to be migrated from classical encryption.
- **Impact:** HHS was able to have a comprehensive cryptographic inventory of their high value assets ahead of the OMB's deadline and successfully removed the identified vulnerabilities to strengthen supply chain cybersecurity.



Learn About Solutions

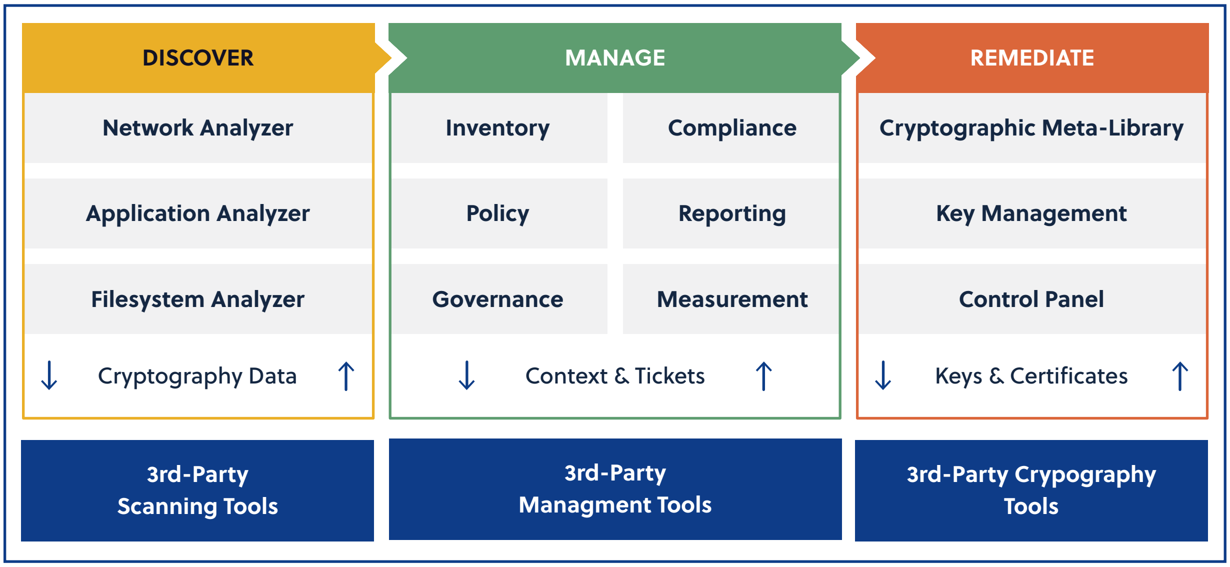
As quantum technology rapidly advances, organizations must prepare for its profound impact on cybersecurity, computing, and data protection. Quantum computing introduces both unprecedented opportunities and significant risks, particularly in cryptography, where traditional encryption methods will soon be vulnerable.

To stay ahead, agencies should begin exploring quantum-safe security solutions, including Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Random Number Generators (QRNG). This section takes a deeper dive into how quantum-driven products and solutions are shaping the future of data security, risk management, and computational power, ensuring resilience against emerging quantum threats.

SANDBOXAQ

Sandbox: AQtiveGuard

SandboxAQ AQtive Guard Architecture



DISCOVER

Network Analyzer

Application Analyzer

Filesystem Analyzer

↓ Cryptography Data ↑

MANAGE

Inventory

Compliance

Policy

Reporting

Governance

Measurement

↓ Context & Tickets ↑

REMEDIATE

Cryptographic Meta-Library

Key Management

Control Panel

↓ Keys & Certificates ↑

3rd-Party Scanning Tools

3rd-Party Managment Tools

3rd-Party Crypography Tools

Transforming the World with AI and Advanced Computing

AQtive Guard provides valuable insights into your cryptography usage. Our analyzers capture snapshots of your cryptography triggered by your automated workflows, **ensuring real-time visibility of your cryptographic inventory at intervals of your choice**. By compiling information from three types of analyzers, AQtive Guard delivers comprehensive 360-degree visibility into your organization's cryptographic inventory:

NETWORK ANALYZER

Captures network traffic and identifies cryptography used to protect data in transit.

APPLICATION ANALYZER

Detects all calls to cryptographic libraries made by an application at run time, identifying vulnerabilities and policy breaches.

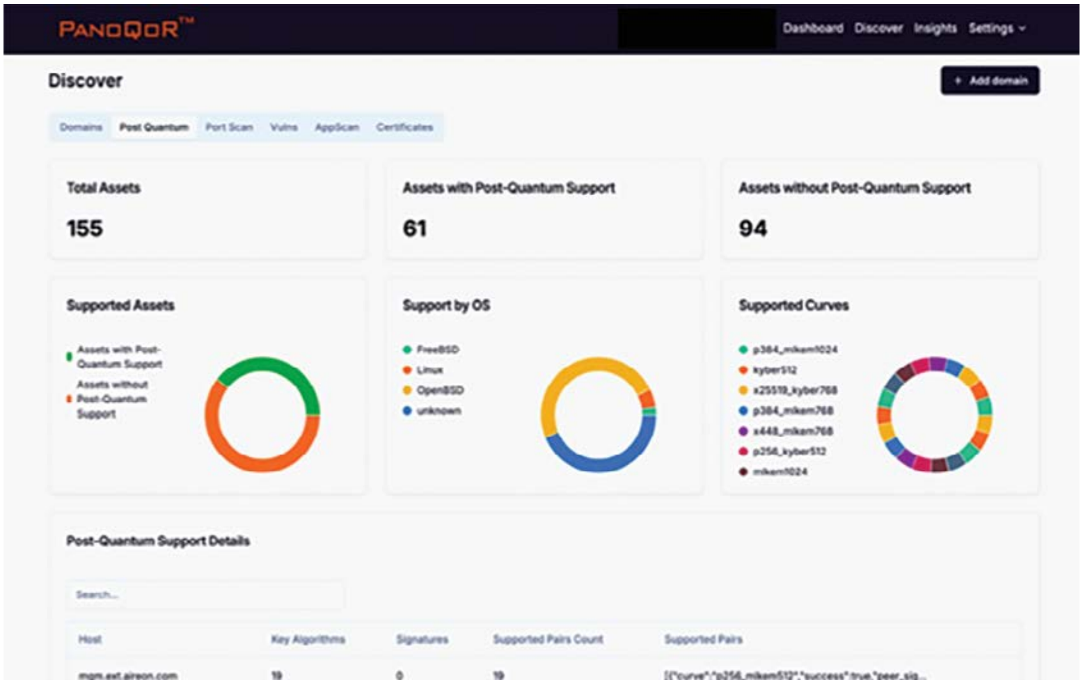
FILESYSTEM ANALYZER

Scans files to find and parse cryptographic artifacts in data at rest.

PATERO
QUANTUM SECURE COMMUNICATIONS

Patero: PanoQoR

PanoQoR™ integrates network scanning with advanced analytics to guide organizations in developing data-driven cryptographic migration strategies. It also detects quantum-vulnerable cryptography securing critical operations, as well as embedded cryptographic elements within internal systems and products.



Total Assets 155

Assets with Post-Quantum Support 61

Assets without Post-Quantum Support 94

Post-Quantum Support Details

Host	Key Algorithms	Signatures	Supported Pairs Count	Supported Pairs
mgm.ext.aireon.com	19	0	19	[{"curve":"p256_mlkem512","success":true,"peer_sig...

PanoQoR begins by discovering and cataloging network domains and subdomains. It then performs port scans, application scans, and retrieves SSL certificate data from network endpoints. Using this data, PanoQoR identifies vulnerabilities such as expired or soon-to-expire certificates, open ports, and misconfigurations. These vulnerabilities are contextualized based on asset criticality and system importance, helping prioritize remediation efforts by cost and impact. The platform also includes analytics that assess and score cryptographic risk in the context of potential quantum computing threats.

The resulting cryptographic inventory, identified vulnerabilities, and quantum risk assessments are compiled into a detailed report provided by Patero's experts.

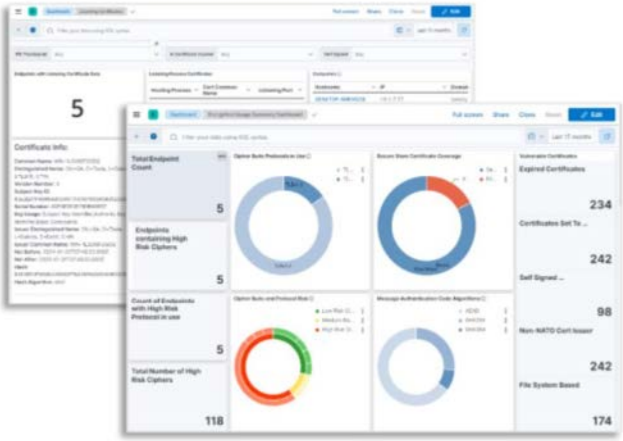
Encryption Discovery & Inventory

TYCHON

Tychon: EndPoint Management System

Capabilities:

- Track certificate by algorithm type
- Identify countries of origin for certificates
- Quickly detect expired certificate
- Calculate certificate ages to identify your most vulnerable certs
- Filter and serarch based on host, keywords, file types, and more



Rapidly gather and inventory cryptography source data across applications, files, and connections. Understand, analyze, and score your risk posture – monitor, trace, and alert on cryptographic inventory changes.

ENTRUST

Entrust: Crypto Health Check

Crypto Center of Excellence (CoE) - Entrust | Identities, secure payments, and protected data

Crypto Health Check—a building block of Entrust CryptoCoE. The Entrust Crypto Health Check arms security, compliance, and risk teams with the tools and expertise required to balance the risks posed by crypto-related threats. We place an expert-by-your-side, recommend best practices, and leverage our unique discovery tools to bring hidden crypto into view.

Crypto Health Check discovery tool scans your environment to build a cryptographic inventory, then scores those findings against cryptography standards and policies. Recommendations for a strong crypto strategy are delivered in a board-ready report. Security, compliance, and risk professionals get all they need to build a CryptoCoE and greatly reduce crypto vulnerabilities throughout their IT ecosystems.

Entrust Crypto Health Check and Crypto Governance Consulting at a glance

✓ Consulting Expert-By-Your-Side

- Security architect
- Crypto policy usage
- Ongoing consulting engagements

✓ Technology Deployed

- Physical scan
- Scans IP/port combinations
- Scans and inventories machines for certificates and crypto
- Scans networks
- Scans for external + internal facing certs
- Evaluates and scores ciphers at endpoints
- Evaluates and scores TLS/SSL portocols

✓ Analyze

- Compliance and auditing
- Evaluates crypto against internal, standard, and quantum policies

✓ Reporting

- Detailed analysis
- Cryptographic inventory
- Crypto readiness
- Compliance recommendations
- Vulnerability scoring
- Health check report
- Recommendations

QuSecure

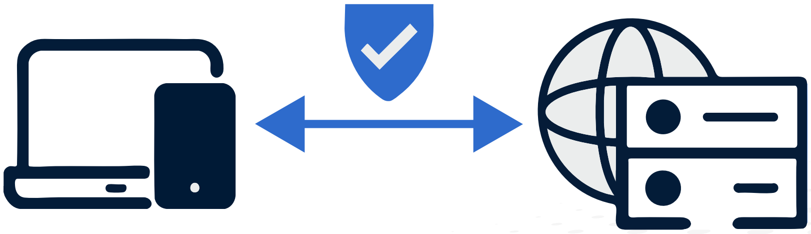
QuSecure: QuProtect

QuProtect offers the ability to upgrade digital infrastructure to quantum-resistant architectures without code change or disruptions to day-to-day operations. QuProtect utilizes initiator and receiver proxies as the fundamental cryptographic unit, creating an additional layer to **protect sessions and data in a post-quantum way** with its patented QSL protocol. By hot-swapping cryptography, the offering provides two independent layers of encryption, with the ability to deploy post-quantum algorithms, enact policy, and modify parameters like key lengths and rotation frequencies through its central management console, QuProtect Orchestrator.

QuProtect supports all NIST PQE Standards and offers the ability to seamlessly swap between algorithms directly through the single pane of glass management console QuProtect Orchestrator. Through its added orchestration layer, QuProtect, in effect, enables classic and post-quantum encryption to work in tandem.

QuSecure's platform consists of three independent products for different use cases:

- **QuProtect Web App Security** for websites and web applications
- **QuProtect Network Security** for network traffic between servers
- **QuProtect Core** for router-to-router communications
    - (Note - QuSecure provides an integrated Quantum Entropy Solution as part of the QuProtect Orchestrator)



quantropi

MASQ™

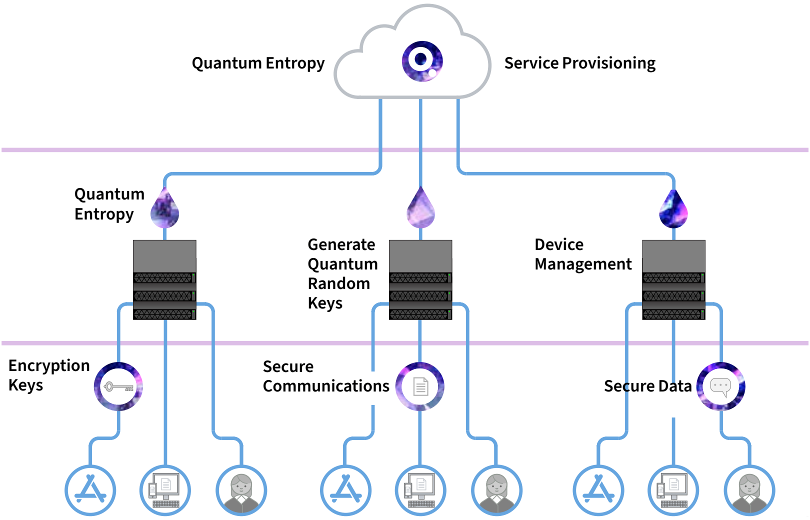
Quantropi: MASQ™

Supports both Asymmetric and Symmetric Encryptions

MASQ™ is a cryptographic library which **supports NIST-approved Post-Quantum Cryptography (PQC) algorithms for both key exchange and digital signatures.**

MASQ™ also features a novel post-quantum cryptographic algorithm developed by Quantropi, designed for resource-constrained devices like IoT. It offers notable performance benefits, such as smaller digital signature sizes, compared to current NIST post-quantum candidates.

This enables customers the flexibility to choose the right algorithm for their needs, and the crypto-agility to change algorithms as the security landscape evolves.



QEEP™

QEEP™

QEEP™ provides enhanced quantum-secure symmetric encryption functionality. Powered by Quantropi's Quantum Permutation Pad (QPP) technology, which achieves Shannon Perfect Secrecy, QEEP™ extends the symmetric encryption key length well beyond the current 256-bit limit. It meets today's security needs and remains safe against future quantum computing attacks, all in a small, efficient, and high-performance package.

Its small code footprint and low computing requirements make QEEP™ the perfect solution to address cybersecurity limitations in resource constrained environments such as IoT and OT devices.

QEEP™ is also high-performance, benchmarked at up to 18x faster than AES-256, which provides a significant advantage where low latency is a requirement such as Connected and Autonomous Vehicles.

QEEP™ can be combined with AES in a FIPS compliant approach to provide defense-in-depth with minimal impact to performance.

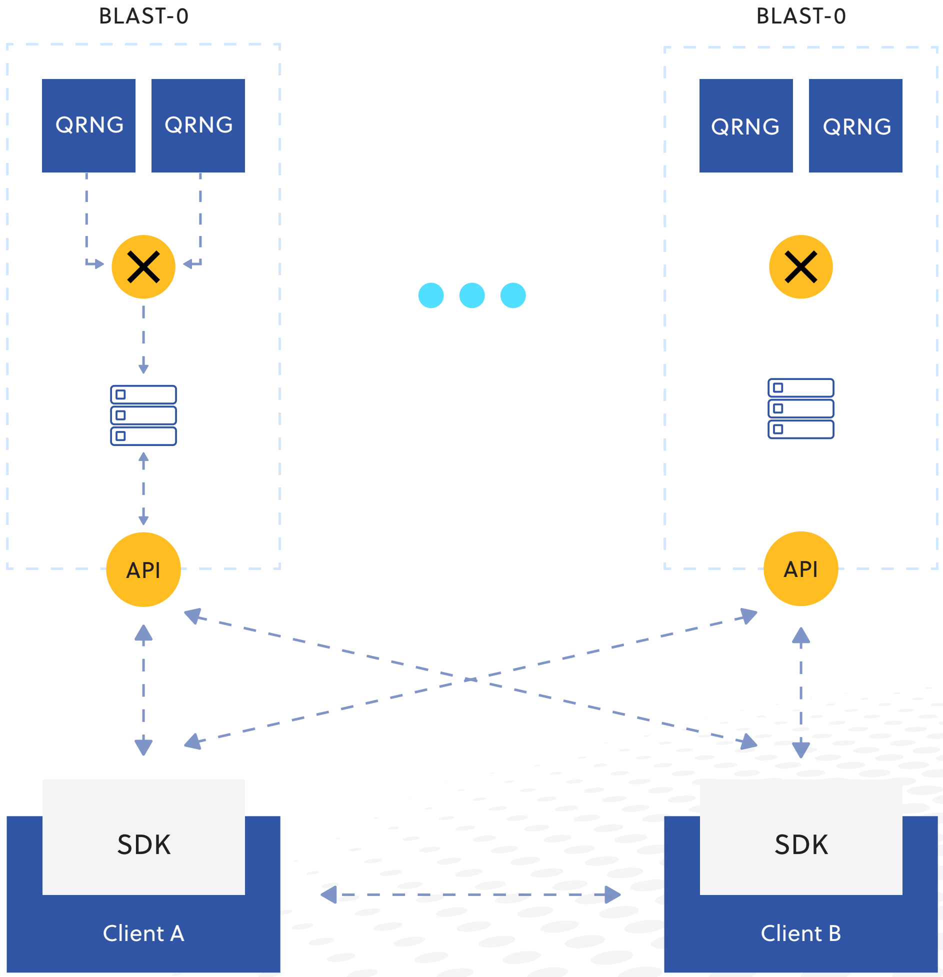
Qrypt

Qrypt's Quantum Key Generation (QKG): BLAST

Key Generation: Qrypt's solution involves generating encryption keys independently at different endpoints using true quantum random numbers, eliminating the need for key transmission

Security: This method addresses the "Harvest Now, Decrypt Later" threat by ensuring that keys are never transmitted and thus cannot be intercepted

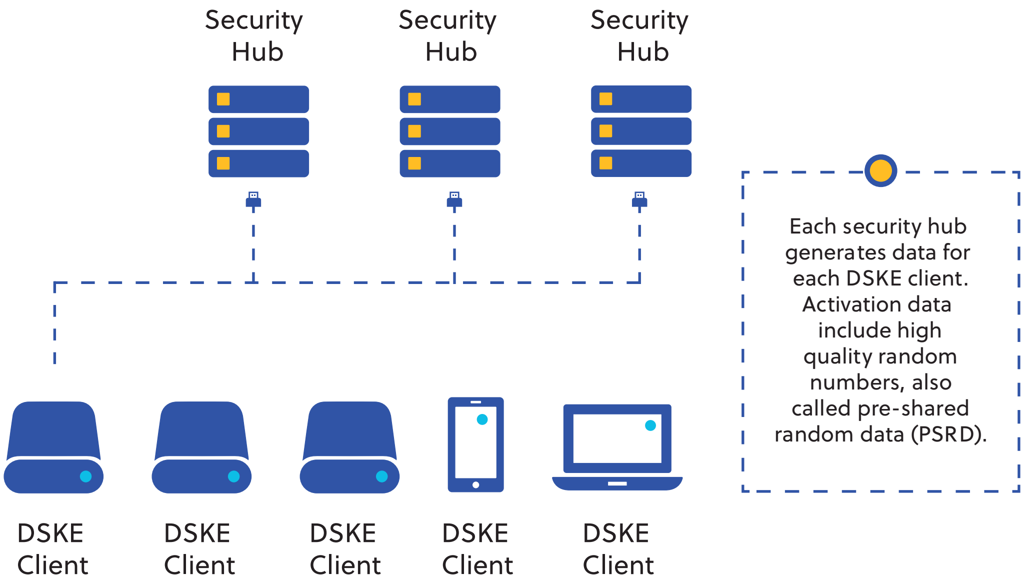
Complementary: Qrypt's QKG can complement NIST PQC by providing an additional layer of security, particularly in scenarios where long-term data confidentiality is crucial.



Quantum Bridge

Quantum Bridge Technologies

Our DSKE products use patented technology that seamlessly integrate into existing infrastructure, delivering quantum-safe, computationally efficient and fully scalable key distribution systems, either for network appliances or endpoint based solutions.



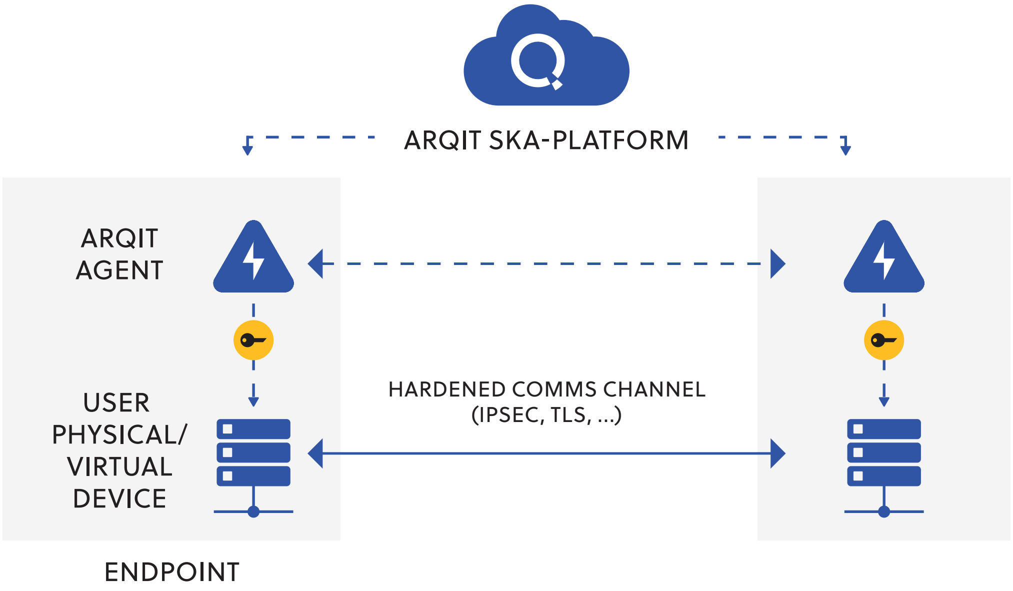
Each security hub generates data for each DSKE client. Activation data include high quality random numbers, also called pre-shared random data (PSRD).

Distributed Symmetric Key Establishment (DSKE) is a scalable, information-theoretically secure key distribution system that can be used with the current internet infrastructure to distribute disposable symmetric secret keys among any group of users. DSKE is provably quantum-secure. The cryptographic keys obtained via DSKE can then be used to protect data at rest or in transit via standard symmetric ciphers and authentication techniques. In case those techniques are information-theoretically secure, the entire communication maintains the same property.

ARQIT

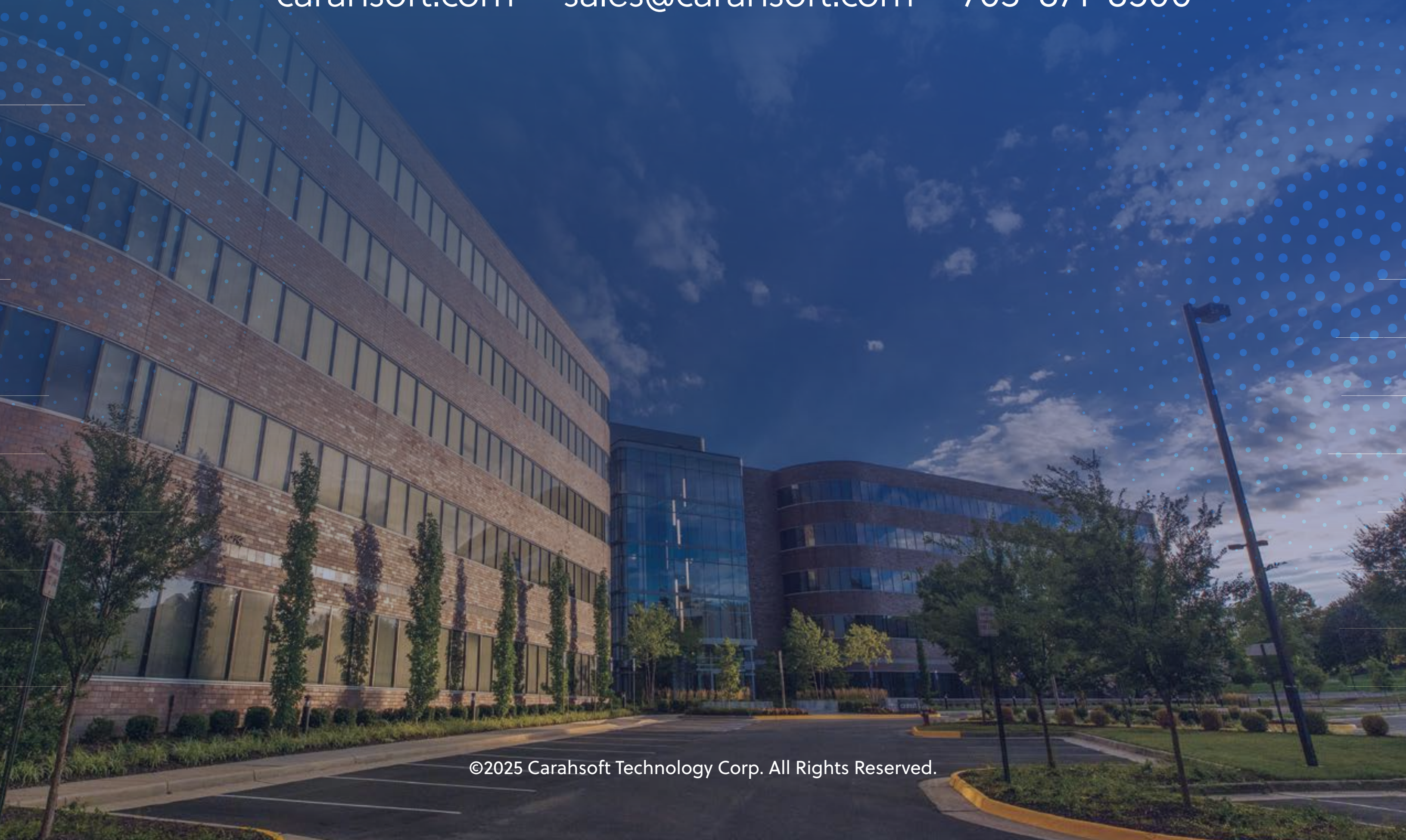
Arqit: Symmetric Key Exchange

Arqit’s SKA-Platform enables quantum-safe communication across connected devices, delivering strong protection against both current and emerging cyber threats. Offered as a Private Instance (PI) or Platform-as-a-Service (PaaS), it provides flexible deployment options to meet diverse security needs.


ARQIT SKA-PLATFORM
ARQIT AGENT
USER PHYSICAL/ VIRTUAL DEVICE
HARDENED COMMS CHANNEL (IPSEC, TLS, ...)
ENDPOINT

Arqit’s symmetric key agreement platform, SKA Platform™ is an on-prem or cloud-based solution that can replace traditional manually couriered symmetric keys with a dynamic and scalable alternative, securing networks with keys that are unbreakable by a quantum computer. This allows endpoints to upgrade the security of communication channels they create, for example adding quantum protection to an IPSec tunnel.

The platform combines the high security of symmetric encryption with the flexibility of asymmetric, both alleviating the logistical pains of manual key delivery and removing the security issues surrounding PKI. Symmetric keys are generated instantly at endpoint devices using true quantum entropy, meaning only the endpoints know the final key, and can be subsequently rotated at high frequency rates to provide enhanced forward secrecy and mitigate against spoofing threats/attacks.



Quintessence Labs

QuintessenceLabs: qOptica™

QuintessenceLabs offers CV-QKD technology with built-in advantages in terms of cost, form factor, and performance:

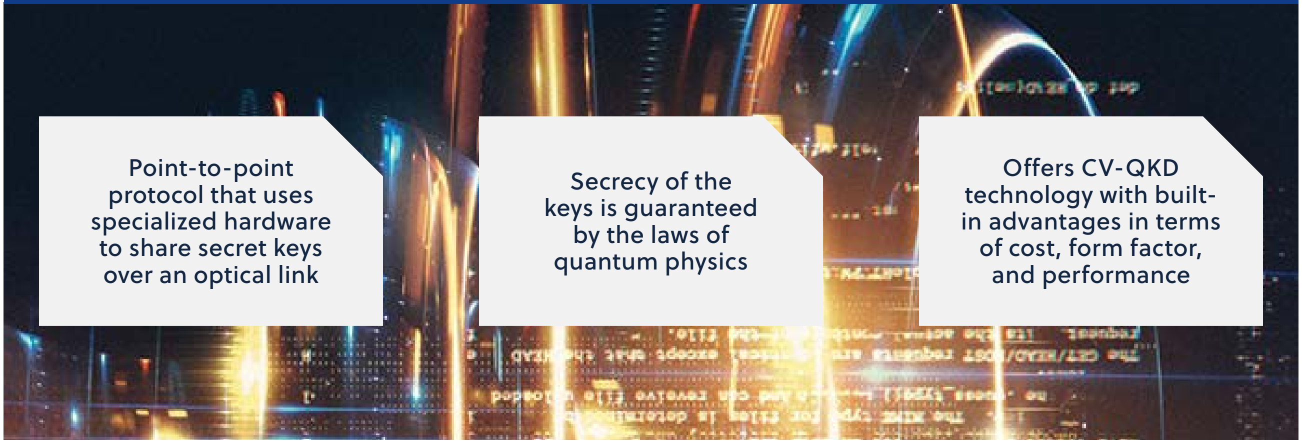
✓ **Performance:**

The use of coherent signal encoding enables high through puts that are not limited by single-photon generation or detection. Moreover, it allows for daylight operation over free space optical links.

✓ **Cost:**

Compatibility with current telecommunication technologies, such as telecommunication encoding, transmission and detection techniques, as well as the ability to use standard fiber connections, allow for cost effective systems.

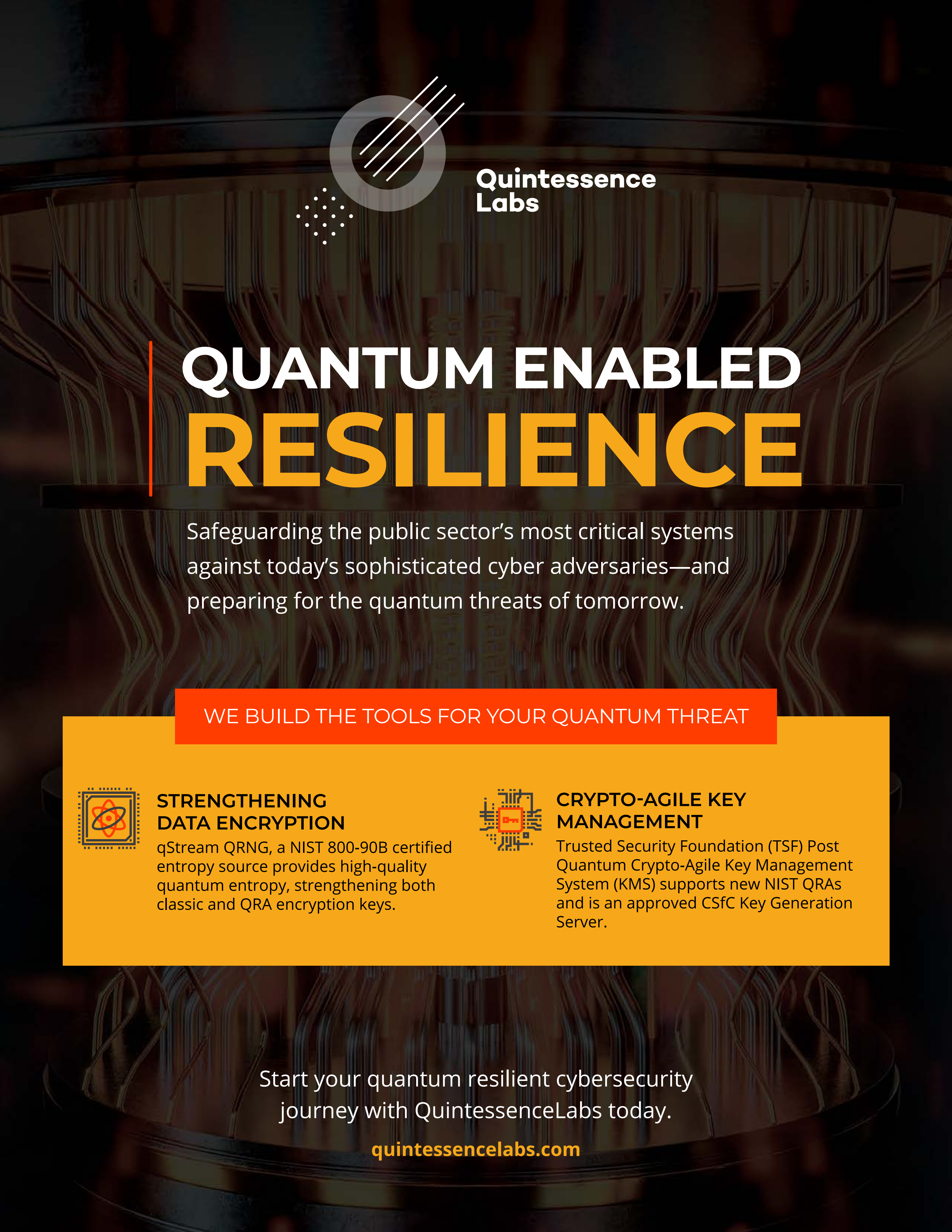
qOptica™ 100 Quantum Key Distribution (QKD)



Point-to-point protocol that uses specialized hardware to share secret keys over an optical link

Secrecy of the keys is guaranteed by the laws of quantum physics

Offers CV-QKD technology with built-in advantages in terms of cost, form factor, and performance



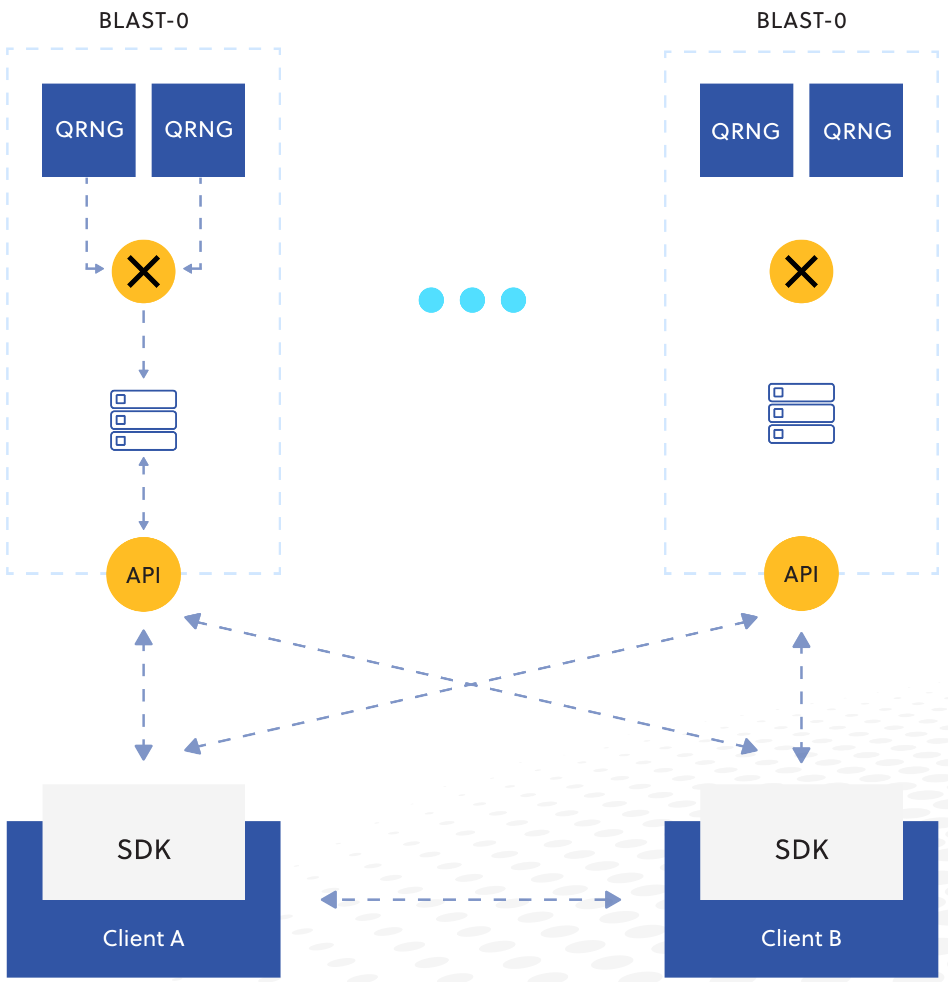
Qrypt

Qrypt's Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is unconditionally secure, even against quantum computers, but is limited in its key rate and communication distance. Furthermore, QKD appliances are still relatively expensive, and they require dedicated optical fibers or line-of-sight free space channel such as ground-to-satellite to work.

Developers need familiar tools based on modern development practices. We provide an SDK that can be easily integrated into applications and infrastructure to make them quantum-secure.

The Qrypt SDK includes client library SDKs, cloud-based REST services, command line clients and guidance to help integrate post-quantum security into your applications and services. You can add security features to your applications without being an expert in post-quantum cryptography.



QUANTINUUM

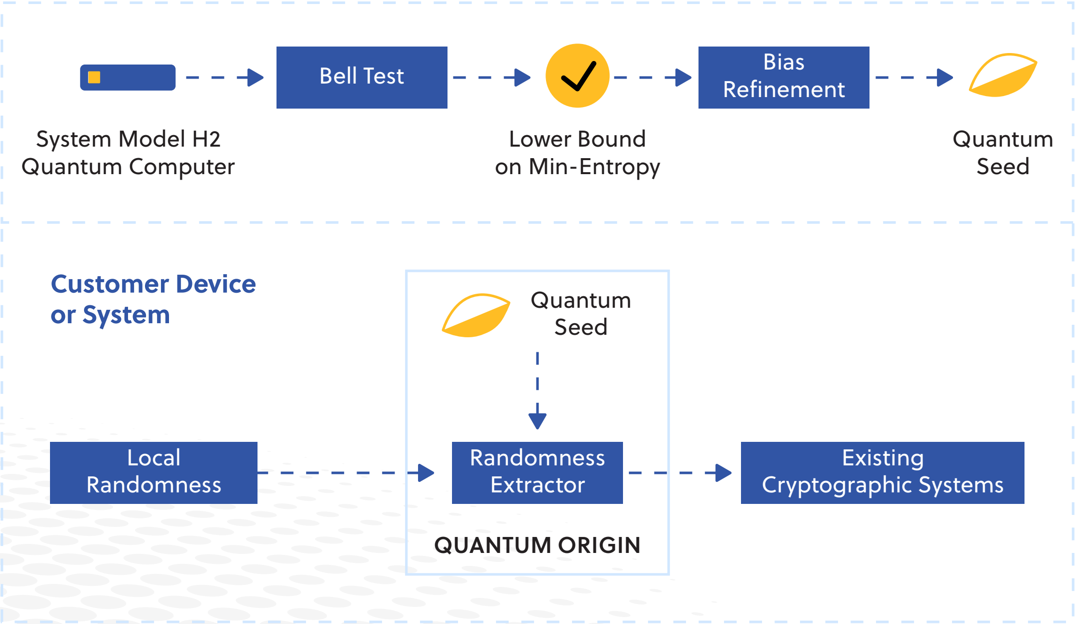
Quantinuum: Quantum Origin

Quantum Origin is the world's only provable and software-deployed quantum random number generator. By integrating Quantum Origin into your infrastructure, you can strengthen the cryptographic keys that protect your most critical data and systems. You can easily deploy Quantum Origin into your existing systems, thanks to our pre-built integrations. Plus, its unique software-based deployment eliminates the need for extra hardware or a cloud connection.

Quantum Origin is a QRNG with three unique technical features:

- The randomness from Quantum Origin is mathematically proven to have a near-perfect min-entropy value, which no other QRNG we know of can achieve. We refer to this as "quantum-enhanced randomness".
- Unlike other QRNGs, Quantum Origin enhances a classical, local source of randomness to produce quantum-enhanced randomness.
- Thanks to the use of randomness extractors, Quantum Origin is deployed as a standalone software module, offering unprecedented scale and ease-of-integration.

At a high-level, the components of Quantum Origin are shown below:



quantropi

QiSpace™ SEQUR provides scalable, high-performance Quantum Entropy as a Service (QEaaS) for the generation and secure distribution of quantum entropy, or true random numbers, to endpoints over existing network infrastructures. Its ease of deployment makes QiSpace™ SEQUR a practical solution to enhance the security of current systems.

Multisource Quantum Physcial Generation

Quantum-Secure Distribution

Entropy Sovereignty

Entropy Expansion

Quintessence Labs

QuintessenceLabs: qStream QRNG

The qStream QRNG delivers random numbers through the industry-standard OASIS Key Management Interoperability Protocol (KMIP), enabling interoperability with any conformant key management server, such as our TSF key and policy manager. Raw entropy, conditioned entropy and random numbers can also be delivered to clients over a standard TCP/IP network connection, or via mutually authenticated TLS at up to 1 Gbit/sec.

Integrating the qStream QRNG appliance into your existing security infrastructure is as simple as installing any other appliance or device in your network:

- The qStream™ 100 Quantum Random Number Generator (QRNG) is a PCIe Gen 2 card that adds true random number generation to existing appliances. It delivers the same full entropy random numbers sourced from two integrated 8 Gbit/sec quantum entropy sources.
- The qStream™ 200 quantum random number generator (QRNG) supports hot-swappable power supplies, fans, and hard drives for straightforward maintenance when needed. Management is performed through a web-based (HTTPS) interface, TLS-protected API calls, or via SSH command line.

qStream QRNG products can also directly integrate with QuintessenceLabs' Trusted Security Foundation® (TSF®) key and policy manager. The TSF key and policy manager is the preferred choice for management of qStream's quantum random number generation, and like qStream applications, supports KMIP and other standards.

Qrypt

Qrypt's Quantum Random Number Generator (QRNG)

Qrypt offers its Quantum Random Number Generator (QRNG) as a standalone product. This QRNG is part of Qrypt's Quantum Entropy cloud service and can be integrated directly with existing infrastructure through a REST API or with integrations for HashiCorp Vault and rngd. This allows customers to use Qrypt's QRNG independently for their own applications.

Qrypt's Quantum Random Number Generator (QRNG) architecture is designed to provide true quantum randomness, which is essential for secure cryptographic applications.

Here are the key components and features of Qrypt's QRNG architecture:

1. Quantum Entropy Source: The QRNG uses quantum fluctuations of optical signals to generate entropy. This method ensures that the randomness is truly unpredictable and not influenced by classical noise.

2. Collaboration with Research Institutions: Qrypt's QRNG technology has been developed in collaboration with leading research institutions like Oak Ridge National Laboratory (ORNL) and Los Alamos National Labs (LANL). These partnerships help enhance the QRNG's reliability and security.

3. Integration and Accessibility: The QRNG can be integrated directly with existing infrastructure through a REST API or with integrations for HashiCorp Vault and rngd. This makes it accessible for various applications and easy to implement.

4. High Data Rates: Qrypt's QRNG architecture supports high data rates, with current capabilities reaching up to 1.5 Gbps. There are ongoing efforts to increase this to 3 Gbps, and ultimately 6 Gbps.

5. Security and Transparency: The QRNG architecture includes measures to filter out classical noise and isolate quantum effects, ensuring the minimum entropy required for true randomness. Qrypt also discloses min-entropy values to ensure trust and verifiability.

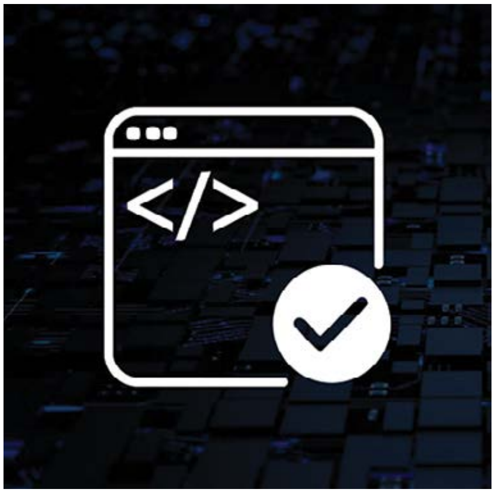
These features make Qrypt's QRNG a robust and reliable solution for generating true quantum random numbers, which are crucial for secure encryption and other cryptographic applications.

CRYPTO4A

Crypto4A: QxHSM™

QxHSM™ architecture is designed to provide quantum-safe, crypto-agile security solutions.

Here are the key components and features:



1. QxTrust Architecture™: This forms the foundation of Crypto4A's HSM, integrating Hardware Security Modules (HSM) with General-Purpose Processing Engines and Confidential Compute Engines.

2. Modular Blade Form Factor: The QxHSM™ is available in a modular blade form factor, which allows for flexible deployment models. It can be used in a single module desktop enclosure, a three-module 1U blade server enclosure, or a high-density ten-module 3U blade server enclosure.

3. Quantum-Safe Cryptographic Agility: The architecture supports quantum-safe cryptographic algorithms, ensuring that the system remains secure against future quantum computing threats.

4. Scalability and Mobility: The QxHSM™ is designed for scalability, allowing multiple blade modules and enclosures to be combined for clustering on a global scale. This ensures high rack density and reduced operational costs.

5. Separation of Duties: The architecture enables true separation of duties, allowing organizations to fully own and control their cryptographic assets, whether leveraging externally managed resources or operating hardware in their own infrastructure.

6. Flexible Deployment: The QxHSM™ supports flexible cloud-scale deployment architectures, adapting to changing markets, standards, and requirements.

These features make Crypto4A's QxHSM™ a robust solution for organizations looking to secure their digital assets in a post-quantum world.

THALES

Thales TCT: Quantum HSM

The Thales TCT Quantum HSM (Luna T-Series HSM) is an advanced hardware security module designed to provide enhanced cryptographic security by leveraging quantum technologies.

Here are some key features:

1. Quantum Enhanced Keys: The Thales Quantum HSM integrates a Quantum Random Number Generator (QRNG) chip, which produces high-quality entropy. This ensures that all random numbers and cryptographic keys generated by the HSM are of the highest quality.

2. Post-Quantum Cryptography: It supports Quantum Resistant Algorithms (QRAs) to protect against future quantum cyberattacks. This makes it suitable for organizations looking to future-proof their cryptographic infrastructure.

3. Compliance and Security: The Thales Quantum HSM is FIPS 140-2 Level 3 compliant, ensuring it meets stringent security standards.

4. Integration: It can be integrated with existing Thales HSM solutions, providing a seamless upgrade path for organizations looking to enhance their cryptographic security with quantum technologies.

THALES

Building a future we can all trust

Post-Quantum Readiness Begins with Crypto Agility

Thales Trusted Cyber Technologies' crypto-agile solutions enable you to future-proof your agency. Our products have been purposely designed to help your agency be quantum-safe:

- **Flexible.** Quickly change protocols, keys, and algorithms.
- **Proactive.** React timely to cryptographic threats.
- **Strategic.** Minimize disruption with advanced technology.

Learn more at thalestct.com.

Contract Vehicles

Carahsoft offers a number of contract options for purchasing Quantum solutions. Our contracts offer purchasing options for civilian, defense, education, state, and local government customers. Customers can purchase solutions off of these major contract vehicles:

GSA Multiple Award Schedule (MAS)

Carahsoft holds a GSA Multiple Award Schedule (MAS) that allows customers to procure a wide variety of Quantum solutions. Carahsoft holds Contract #47QSWA18D008F and allows customers to purchase everything from identity to automation & orchestration solutions.

ITES-SW2

The purpose of the ITES-SW2 acquisition is to support Army, Department of Defense (DoD) and all Federal Agency enterprise Information Technology (IT) infrastructure and info-structure goals by leveraging Commercially available-Off-The-Shelf (COTS) software products and maintenance in 14 product categories in addition to related incidental services and hardware.

NASA SEWP V

The NASA SEWP V GWAC (Government-Wide Acquisition Contract) provides the latest in Information Technology (IT) products and product-based services for all Federal Agencies. SEWP provides the best value and cost savings through innovative procurement tools and processes; premier customer service and outreach; and advocation of competition and cooperation within the industry.

NASPO ValuePoint Cooperative Purchasing Organization

The NASPO ValuePoint Cooperative Purchasing Organization (formerly WSCA-NASPO) provides the highest standard of excellence in public cooperative contracting. By leveraging the leadership and expertise of all states with the purchasing power of their public entities, NASPO ValuePoint delivers best value, reliable, competitively sourced contracts.

Since 1993 NASPO ValuePoint has been the cooperative purchasing arm of NASPO (the National Association of State Procurement Officials) encouraging, fostering and guiding the nation's most significant public contract cooperative. NASPO ValuePoint is a unified, nationally focused cooperative aggregating the demand of all 50 states, the District of Columbia and the organized US territories, their political subdivisions and other eligible entities spurring best value, innovation and competition in the marketplace.

OMNIA, Partners – Cobb County

Carahsoft holds an OMNIA Partners, Cobb County, GA Technology Products, Solutions and Related Services contract (#23-6692-01) that provides full access to a portfolio of value-driven contracts, spend visibility analytics, and subject matter experts.

OMNIA Region 4 – Education Software Solutions and Services

Carahsoft Technology Corp., The Trusted Government IT Solutions Provider®, been awarded a Region 4 Education Service Center (ESC) contract (#R191902) for Educational Software Solutions and Services available now through OMNIA Partners. This contract makes these solutions available to state and local government agencies, education institutions, non-profits, municipalities, and additional public sector organizations through Carahsoft and authorized reseller partners.

Educational Software Solutions and Services are available through this contract and Carahsoft's reseller partners to public sector organizations in all 50 U.S. states and the District of Columbia, and the contract is established for a five-year period of performance through April 30, 2025. All solutions on this contract are offered at special discounts off their manufacturer list price, and additional price reductions can be provided on a deal-by-deal basis.

Solutions from more than 200 providers are available through the OMNIA contract, encompassing:

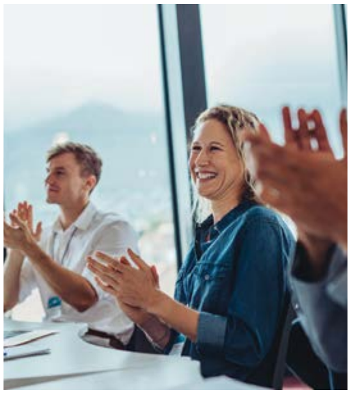
- Software Licenses
- Product Support
- Maintenance Services
- End User Computing
- Cloud Subscription Services
- Training
- Professional Services

Upcoming Quantum Events

★ Marquee Event

GovExec Federal Quantum Summit

August 27, 2025 | Carahsoft Conference & Collaboration Center



Quantum technologies are poised to enact profound transformations across national security and defense. Quantum computing has the potential to crack complex problems that are far beyond the capabilities of current computers, enabling faster decision-making and more effective strategies. For instance, Quantum enabled communication will safeguard critical information against cyber threats with unprecedented security while quantum enabled sensing improves the detection of hidden objects, underwater threats, and even stealth aircraft with astonishing accuracy. Quantum enabled technologies are not just incremental improvements—they represent a leap forward that could redefine the very nature of defense.

Join Nextgov/FCW and Defense One as we convene top government leaders to discuss the current state of quantum computing, how they are innovating and investing, and the future of computing and how it can become the backbone of next-generation military capabilities, ensuring superiority in an increasingly complex and unpredictable world.

Quantum World Congress

September 16-18 | Tysons, VA

Quantum World Congress gathers the world's quantum ecosystem to bring a quantum-ready future into focus. It's the world's premier gathering for quantum technology leaders, innovators, and visionaries. Attend groundbreaking keynotes, engage in cutting-edge discussions, and experience unparalleled networking. This annual event fosters collaboration and accelerates the development of the global quantum ecosystem by highlighting the pivotal role of quantum technology in shaping the future.

NIST 6th PQC Standardization Conference

September 24-26, 2025 | Gaithersburg, MD

NIST published the first three post-quantum cryptographic standards in August 2024, and work continues on additional standards to protect against future quantum computers. Building on this progress, NIST will host the 6th PQC Standardization Conference, bringing together stakeholders from academia, industry, and government, as well as submission teams from the candidates under evaluation, for in-depth discussions and collaborative engagement. This conference will foster a workshop-style atmosphere to support the ongoing development and refinement of the PQC standards.

Q+AI 2025

October 19-21, 2025 | Museum of Jewish Heritage, NYC

Uncover the coming wave of quantum & AI during this 3-day event with 50+ speakers and daily mentoring sessions. Learn about AI use cases to enhance quantum hardware and software design, quantum workflow, and integration in the chip industry at the interface of AI and quantum processing.

Q+AI 2.0 2025 will highlight current applications and future use cases in these fields:

- Automotive
- Aerospace
- Defense
- Robotics
- Supply chains
- Data centers
- Security/Privacy
- Healthcare

Q4I 2025

November 4-6 | Rome, NY

Dive into cutting-edge trends driving quantum technology forward and discover the tools and techniques redefining how we tackle complex challenges. Gain unique insights from leaders across government, industry, and academia, and engage in thought-provoking discussions that push the boundaries of possibility.

Be part of the action during live exchanges with keynote speakers and forge connections that can spark lasting collaborations.

IEEE Quantum Week 2025

August 31 – September 5, 2025 | Albuquerque, NM

IEEE Quantum Week — the IEEE International Conference on Quantum Computing and Engineering (QCE) — bridges the gap between the science of quantum computing and the development of the industry surrounding it. This event brings a perspective to the quantum industry that differs from strictly academic or business conferences.

IEEE Quantum Week is a multidisciplinary venue that gives attendees the unique chance to discuss challenges and opportunities with quantum researchers, scientists, engineers, entrepreneurs, developers, students, practitioners, educators, programmers, and newcomers.

carahsoft

Contact Us:

(844) 214-4790
QuantumComputing@carahsoft.com

11493 Sunset Hills Road, Suite 100
Reston, Virginia 20190

carah.io/quantum