Patero C6ISR Solution Brief

Introduction

Patero's high performance data security products defend critical infrastructure against today's advanced and future quantum computing powered cyber-attacks.

Patero products and solutions are powered by CryptoQoR™ (QoR), a highly efficient crypto module that blends traditional and quantum-resilient algorithms.

QoR quickly and easily deploys into a broad range of existing devices (e.g. microcontrollers, gateways, cloud nodes) to deploy scalable, unified security architectures that keep sensitive information safe and private.

Patero's CryptoQoR is a key component of modern security architectures that simplifies communication networks, provides protection against quantum computer attacks, and address the needs for true C6ISR zero-trust decentralized architectures now and in a post-quantum world.

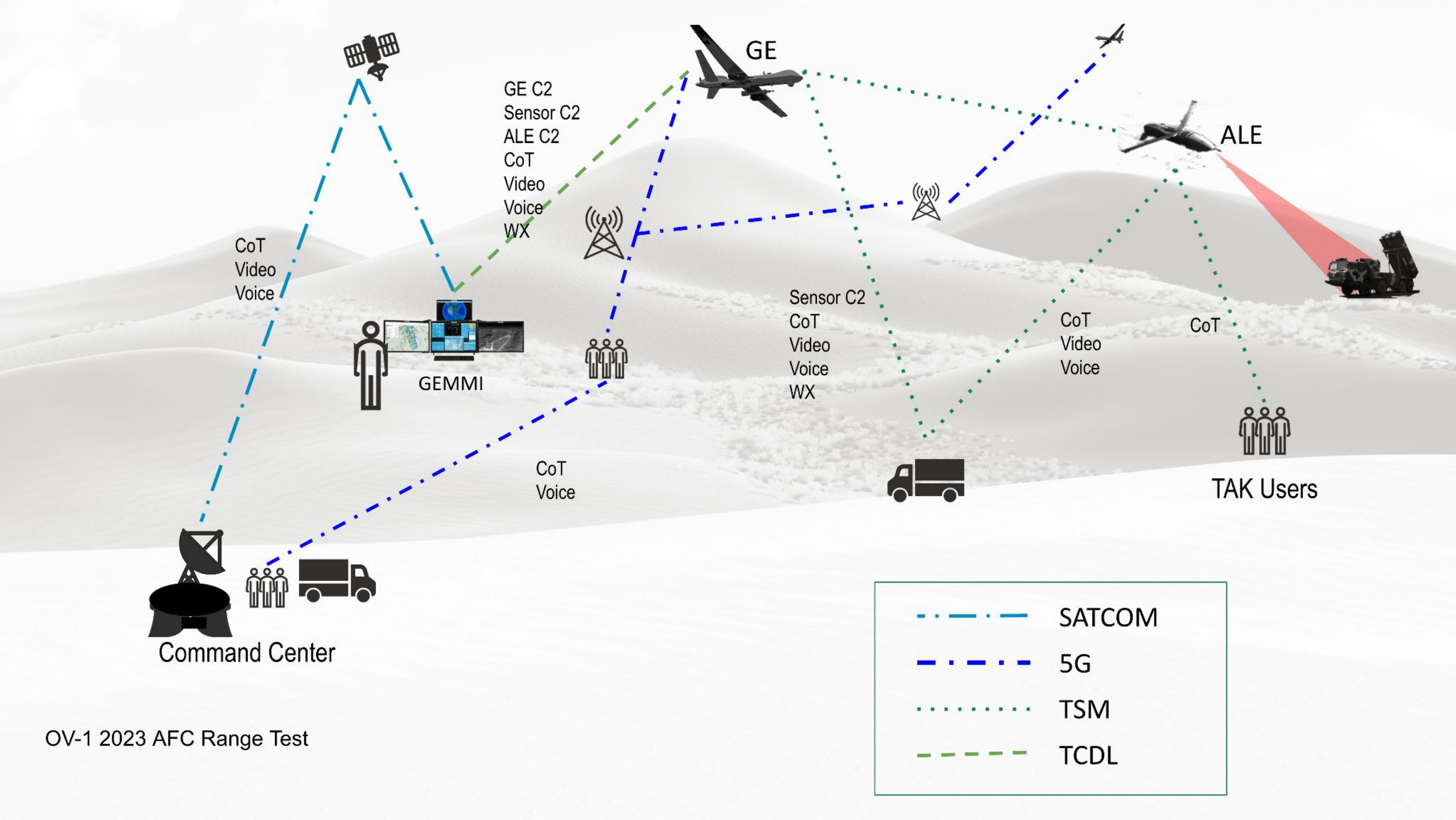
Boeing MQ-25 Stingray

Patero is committed to securing superior operational awareness for warfighters.

Patero CryptoQoR ("QoR") is a software-based crypto module for cloud, edge bare metal, IoT Edge endpoints, or on microcontrollers embedded into systems like UAV platforms and related connected devices. QoR provides the hybrid classic and post-quantum encryption of data in motion for safe transmission of sensitive information between assets and across security boundaries.

The QoR engine is uniquely suited to securely optimized data flows across the C6ISR infosphere Patero's crypto-agile solution runs in kernel space of the host operating system consuming minimal overhead and latency thus able to support real-time communications with the edge. QoR hybridizes today's classic encryption NIST post quantum encryption algorithms.

The CryptoQoR solution is inherently Zero Trust - ensuring that endpoints must present quantum-derived mission keys for authentication. Crypto-agility enables algorithm selection for each or all communication legs via a centralized configuration and monitoring console.



OV-1 2023 AFC Range Test

Solution

Patero QoR is a quantum-secure, end-to-end encrypted solution providing ultra-secure, granular access to specific C6ISR resources for actionable warfighting measures.

Transmission safety is guaranteed by using hybrid PQC (Post-Quantum Cryptography in combination with today's standard encryption). Access control between endpoints is ensured by validating quantum keys (symmetric and session keys) and other measures.

The ability to deploy containerized applications to target endpoints enables evergreen lifecycles and dynamic adaptation to a changing threat landscape by adding features like device, user and application authentication to enable zero trust capabilities without weakening the underlying base security.

Solution Technical Components

1. Patero QoR End-to-End Crypto Software Engine - Linux Server Version
2. Patero QoR - Edge version
3. Patero Secure Network Operations Management Console “Qorsight”- Enables customers to configure and manage QoR Deployments, and to maintain the system over the service life.

Solution Deployment Steps

1. Sign Patero License
2. Deploy and Setup the basic secure network virtual private cloud “QoR Server”
3. Deploy and Setup the basic secure network operation management console “Qorsight”
4. Deploy Patero QoR on each of the targeted end-points.
5. Test and Verifications
6. Training by the Patero staff engineering team and hand-over for pre-field operations/demo
7. Qorsight Enhancements subject to discussion and NRE

Feature 1 Hybrid

Challenge:	Attribute:	Benefits:	Business Impact:
NIST has cautioned that any encryption algorithm may be broken in the future with advances in quantum computing and code breaking algorithms. That is why NIST recommends a hybrid approach combining classical with new quantum-resistant encryption.	Patero QoR combines trusted classical and NISTs newly available quantum-resilient crypto-algorithms. By hybridizing the keys from these two algorithms, Patero CryptoQoR creates an ultra-secure encrypted data stream.	QoR is a pragmatic PQE option that retains classic encryption and hybridizes it with post-quantum encryption. The Patero result is “double wrapping” - meaning the bad guys would have to break both encryption schemes to get to the goods.	The bad guys are stealing data today planning to decrypt it later (SNDL). Hybrid PQC allows immediate mitigation of data loss by protecting it today with existing classical encryption and also protecting it with post-quantum encryption from being decrypted tomorrow.

Feature 2 Crypto-agile

The term crypto-agility typically refers to system design that is flexible, enabling customers to immediately adopt new cryptographic algorithms with zero impact and maintaining zero trust within ongoing operations.

Challenge:	**Attribute:**	**Benefits:**	**Business Impact:**
As PQC standards evolve, network operators will have to figure out how to accommodate differences in key sizes, encrypted file sizes and signature lengths across billions of devices and miles of infrastructure, without compromising the value of digital systems. Without a crypto-agile solution, those administrators are left without truly viable cost-effective PQE deployment options.	QoR's modular design enables users to select and switch cryptographic algorithms, regardless of scheme diversity, through an easy one-click mechanism.	Critical infrastructure is continuously protected as attacker creativity and quantum standards evolve	Especially in operations that are geo-distributed, autonomous and sensor-dense, operators can move from planning to implementation phases of PQC migration without worrying about future threat vectors and cryptographic standards. Upgrades can be performed with minimal impact on operations. Customers can also select algorithms, regardless of scheme diversity, to customize for operational requirements.

ROI: Continuous protection enables infrastructure operators to protect existing infrastructure now, thus extending asset lifecycle. Crypto-agility also eliminates the need to rip and replace both assets and security infrastructure as threat vectors and standards evolve.

Feature 3 Efficient

Challenge:	Attribute:	Benefits:	Business Impact:
Quantum-resistant cryptography can be heavy and can compromise operations that depend on communications that are urgent, are received in near real time, or support operations that are sensitive to timing.	QoR is lightweight and multi-threaded to support high throughput and sub-millisecond latency.	QoR is designed to operate on a broad range of compute options including microcontrollers, ARM, x86, RISC, and GPU cores to deploy scalable unified security architectures that enable secure communications wherever they are needed (M2M, B2B, V2X, E2C, mobile phones, satellite, etc.).	Customer-defined security architectures support data sovereignty initiatives, reduce attack surfaces, prevent data leaks and enable customers to trust data and networks. When enterprises can use networks without fear, they can fully realize the benefits of their data and other digital assets.

QoR uses Quantum key derivation mechanisms to create session keys that enable Quantum secure communication even in challenging environments with low bandwidth or high packet loss.

Customers can:

- Deploy technology on all physical and digital assets to create unified, customer-defined **security architectures**
- Use trusted channels to share information with outside entities
- Ensure data integrity for environments dependent on near real-time data exchange

Feature 4 Enterprise-grade (ready to deploy)

Challenge:	Attribute:	Benefits:	Business Impact:
Some solutions involve lengthy, complicated deployment and optimization processes	Field-proven QoR solutions are rapidly deployed where needed (e.g. bare metal, cloud, edge gateways) to enable quantum-resilient networks and zero-trust architectures	QoR can be deployed immediately to protect critical assets without disruption to operations or process. QoR is architected such that it will protect device/network node application containers	Operators can take full advantage of their digital resources while protecting physical assets and process from command and control attacks, steal now/decrypt later, and eavesdropping

Feature 5 Standards-based

Challenge:	Attribute:	Benefits:	Business Impact:
NIST standards are not yet established and will evolve over time	Hybrid cryptography will always contain certified algorithms combined with NIST-qualified candidates	Patero's hybrid cryptography improves, not replaces, current security, ensuring that customers can deploy quantum-safe cryptography while remaining compliant (e.g. NIST, FIPS 140-2) now and as standards evolve	Customers can avoid lengthy procurement cycles to start PQC migration before quantum computing is fully mature and available to threat actors.

ROI: Peace of Mind