PATERO
QUANTUM SECURE COMMUNICATION

Quantum-Resistant Red Hat Enterprise Linux

Keep your secrets
Trust your network
Stay ahead of the bad guys

Red Hat
Business Partner

TODAY'S ENCRYPTION IS OBSOLETE

Using Shor's algorithm, Quantum computers will decrypt data encrypted with asymmetric algorithms (RSA, Elliptic Curve). Your data is no longer safe.

Important long-life data is being stolen by bad actors today to be decrypted tomorrow (steal now, decrypt later attacks) when they get their hands on cryptographically relevant quantum computers.

RHEL WITH PATERO FUTURE-SAFES YOUR DATA

Patero's CryptoQoR highly efficient crypto-agile software module for Red Hat Enterprise Linux generates quantum-safe public-private key pairs using NIST post-quantum cryptographic methods. CryptoQoR will also negotiate and generate quantum-safe symmetric keys for standard applications.

CryptoQoR on RHEL provides end-to-end, hybrid post-quantum encrypted communication channels leveraging kernel-based multithreaded encryption. This high-performance, low latency, quantum-safe connectivity protects data-in-motion, retaining traditional encryption protection as the efficacy and resilience of quantum-resistant encryption evolve.

PATERO REDUCES NETWORK ATTACK SURFACES

CryptoQoR enables Zero Trust architectures. Patero CryptoQoR endpoints will only acknowledge connection requests from other Patero-protected endpoints. Authenticated connection pairs are segmented by quantum-safe key assignments. Private quantum-safe and traditional keys are used to authenticate endpoints and provide perfect forward secrecy by frequently rotating newly created quantum-safe session keys.

Hybrid Encryption

CISA, BSI and NIST advocate for "hybrid" post-quantum cryptography. Patero hybridizes classic encryption with NIST standardized post-quantum-encryption.

Cryptoagile

CryptoQoR's modular design enables users to select and switch cryptographic algorithms

Standards-based

CryptoQoR combines today's trusted encryption with NIST candidates for quantum-resilient algorithms.

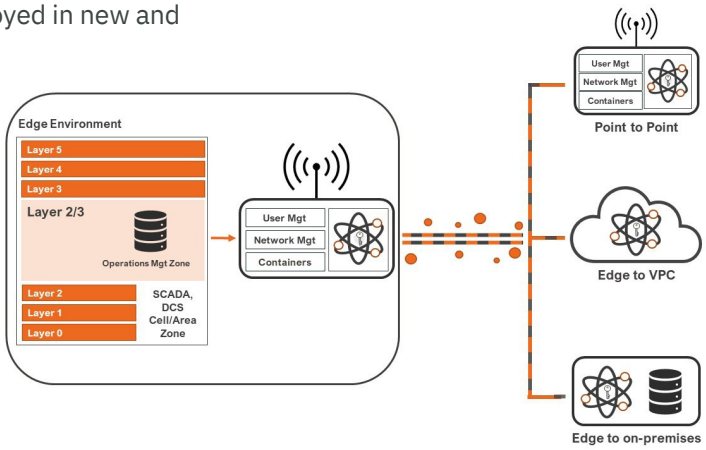
Ready to deploy

CryptoQoR leverages kernel-based symmetric encryption on a broad range of compute options including EDGE gateways, bare metal, VM's, cloud and mobile devices allowing for unified security architectures that protect critical assets without rip and replace.

Deployment Topologies

CryptoQoR is software-based cryptography technology that establishes ultra-secure channels between defined endpoints to protect communications and data in transit from today's advanced attacks and tomorrow's quantum-based attacks. CryptoQoR is hardware-agnostic, can be deployed in new and existing assets and works in a broad range of compute options. The most common deployment topologies are:

- **Point to Point** - one-to-one channels transmitting sensitive, classified or personal data.
  Example: MPLS replacement
- **Multipoint to Point (EDGE-to-Cloud)** - communication from multiple assets and/or locations to virtual private cloud or private cloud.
- **Multipoint to Point (on-premises)** - communication from multiple assets to a central, on-premises server.
  Example: Video surveillance cameras to camera server



Specifications

Supporting Operating Systems

x86 based systems:
- RHEL 9
- Oracle Linux 9 UEK
- SLES 15
- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Debian 11
- Debian 12
- Yocto Linux

ARM based systems:
- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Raspbian 10
- Raspbian 11
- Raspbian 12

Recommended Edge Endpoint Configuration

CryptoQoR supports ARM and x86 endpoints:
- 1 GHz CPU
- 1 GB RAM
- 1 network interface

Supported network types are physical ethernet interfaces including WiFi, 4G / 5G, satellite connectivity.

Recommended Cloud Endpoint Configuration

CryptoQoR supports cloud-based VM's and bare metal
- 2 GHz CPU, 4 cores
- 4 GB RAM
- 2 network interfaces

CryptoQoR supports standard VMWare, KVM, Hyper-V and OpenStack virtual interfaces. CPU and memory requirements depend on the desired throughput and latency.

Performance (*)

- Latency: < 1 msec
- Bandwidth: 99%
- CPU Load: < 5%

* Typical performance of CryptoQoR encryption observed in Oracle Cloud Infrastructure. Performance may vary in your environment and depends on many factors like throughput, MTU size, CPU performance etc.

CryptoQoR protects communications by cloaking internet- facing network elements and using hybrid post- quantum encryption to improve today's encryption.

Please visit www.patero.io

EMEA
Patero GmbH
Feldstraße 15
29386 Hankensbüttel
GERMANY
+49 151-16246830
quantumsafe@patero.de
www.patero.de

North America
Patero Inc.
7757 Baltimore Ave, Suite 1603
College Park, MD 20742
U.S.A
+1 650-641-0678
quantumsafe@patero.io
www.patero.io

PATERO
QUANTUM SECURE COMMUNICATION