ORACLE | Partner

Quantum Resistant Oracle Linux

Cloak and Secure Data-in-Motion, Edge-to-Cloud

Oracle Partner

PATERO
QUANTUM SECURE COMMUNICATION

"My experts and I spent days looking for Patero-cloaked Internet-facing endpoints. We couldn't find them. Patero hybrid post-quantum is the real deal and puts the bad guys on their heels."

Pete Clay,
CISO Airon LLC.

Patero's CryptoQoR™ crypto module for Oracle Linux cloaks exposed network endpoints from discovery by cyber criminals and encrypts data-in-motion with hybridized cryptographic keys derived from classical encryption and NIST's post-quantum cryptographic algorithms.

CryptoQoR on Oracle Linux 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, combining NIST post-quantum cryptography with classic encryption protection to ensure present and future cryptographic resilience.

Executive summary

Patero for Oracle cloaks Internet-facing network elements and makes data indecipherable with quantum-safe encryption. Patero's solution delivers end-to-end protection for critical infrastructure and federal and DoD networks. Patero's product suite helps enterprises identify and remediate immediate network and future cryptographic vulnerabilities. Its hybrid post-quantum security solution uses today's best encryption technology hybridized with NIST's next-generation quantum resilient encryption algorithms.

Product profile

Cloak Cloud Gateways running on Oracle Linux

Bad actors scan for responsive ports. Once detected, the attack begins. Just as a black hole doesn't reflect light, Patero-protected cloud gateways don't respond to requests of any kind EXCEPT from trusted, known, Patero-protected network elements. Patero-protected endpoints form a Zero-Trust network establishing quantum-resistant data channels using hybrid classic and post-quantum encryption.

Oracle Linux with Patero Future-Safes Data against Quantum Attacks

- The encryption you are using today is already obsolete. NIST has already deprecated RSA 1024 and pre-announced deprecation of RSA 2048. Classic encryption can't stand up to quantum computers using Shor's algorithm. Asymmetric crypto-systems such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) must be replaced.
- Make your data future-safe! Important long-life data is being stolen today because the bad actors can decrypt it in the future with cryptographically relevant quantum computers. Patero for Oracle Linux protects sensitive data today and into the future.
- Patero's hybrid post-quantum security solution employs today's best encryption technology hybridized with NIST's next-generation quantum resilient encryption algorithms to make data indecipherable with quantum-safe encryption. Patero's solution delivers end-to-end protection for critical infrastructure, federal, and DoD networks.

Product benefits

CryptoQoR is a software-based cryptographic module that establishes ultra-secure channels between defined endpoints to protect communications and data in transit against today's advanced attacks and tomorrow's quantum-based attacks.

CryptoQoR with Oracle Linux is fast, light, and easy to install.

- CryptoQoR installs on Oracle Linux with an easy RPM install process with an intuitive Web UI. PQC encrypted traffic between nodes introduces negligible latency and overhead for double-digit Gbps performance.

Quantum-Resistant Oracle Linux is Future Safe: "Crypto-Agility"

- The ability to adopt new releases of cryptographic algorithms without disrupting data flows is called "crypto agility." CryptoQoR for Oracle Linux is crypto-agile. New, more advanced algorithms can be deployed to PQC-enabled Oracle Linux endpoints without interrupting data flows, ensuring continuous uptime and no data loss or impact on operations.

CryptoQoR for Oracle Linux Supports Multi-linux Environments

- Patero CryptoQoR works with Oracle and other Linux distributions enabling edge-to-anything security in Oracle Linux or blended Linux environments.

linkedin.com/company/patero-inc

patero.io

Cloak and Secure Data-in-Motion, Edge-to-Cloud

Quantum Resistant Oracle Linux

ORACLE | Partner

Oracle Partner

PATERO
QUANTUM SECURE COMMUNICATION

Resources

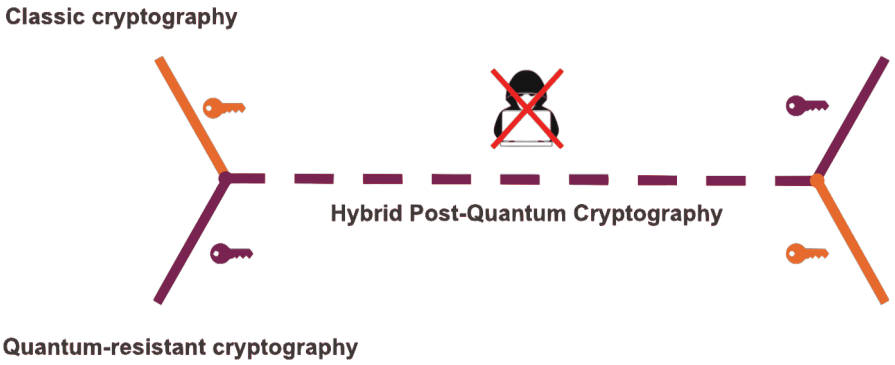
Email:
quantumsafe@patero.io

Phone:
650-641-0678

Peter Bentley
Global Business Executive
Patero Inc

"Exposed Internet endpoints are open invitations to cyber criminals - and critical data classically encrypted moving to the cloud is at risk of being stolen for later decryption by quantum computers. All companies in critical infrastructure will benefit from cloaking and securing data flows with PQC."

Ryan Cahalane
Managing Partner
Axiom Manufacturing Systems



Use cases

CryptoQoR for Oracle Linux is hardware-agnostic, can be deployed in new and existing assets and works in a broad range of compute options from the edge to the cloud.

Common deployment topologies include:

- **Edge-to-Cloud** - securely move data from on-premises sources over the open Internet to cloud resources. Old standards such as TLS are no longer state of the art - and many cloud providers don't even support modern TLS. Patero leapfrogs obsolete asymmetric security like TLS with its NIST-certified post-quantum cryptography.
- **Point-to-Point** - one-to-one channels transmitting sensitive, classified, or personal data. For example, secure transfer of patient records between remote and central medical offices. Patient records are one example of long-life data subject to being stolen now and decrypted later unless post-quantum cryptography is deployed today.
- **IoT/IIoT** - With over 14 billion IoT endpoints in the wild, the bad guys have a big surface to attack. For critical infrastructure and high-value long-life IoT/IIoT data, Oracle with Patero CryptoQoR provides an unmatched level of security, cloaking, and future-safe encryption.
- **Mobile and Inaccessible Assets.** Patero technology remotely monitors and protects petroleum tank farms, ships, and containers at sea, wind, and solar farms. Patero secures remote monitoring and access to physical assets.
- **Electric Vehicle Charging.** Patero technology can protect Electric Vehicle Charging Infrastructure (EVCI) by cloaking and securing L2/L3 chargers.
- **Industrial Manufacturing Processes and Supply Chains.** Patero protects edge-to-cloud operational data. Patero offers ultra-secure and future-safe protection to suppliers across the entire supply value chain.
- **Cybersecurity in Space.** Patero with Oracle can protect data transmitted over free optics technologies.

linkedin.com/company/patero-inc

About Patero

Patero protects the national cybersecurity interests of the United States and its allies. Patero is a network security company that offers civilian and government entities easy-to-use, quantum-resistant future-safe data security products that protect sensitive operational data against cyber threats while maintaining highly resilient, high throughput communication paths. Patero's dual-use products cloak and protect assets, data, networks, and communications vital to critical infrastructure operations.

Learn more quantumsafe@patero.io https://Patero.io