PATERO
QUANTUM SECURE COMMUNICATION

Secure Communications over Insecure Networks

Industry Summary

BACKGROUND

Today, threat actors include hacktivists, criminals, malicious individuals, and adversarial nation states. They target digital systems in national critical functions, not only for monetary gain but also to affect geopolitical and economic stability.

CHALLENGES

Most security technologies were designed to work with fixed systems like datacenters. Modern critical infrastructure includes mobile, decentralized assets often connected to the cloud to enable analytics or remote monitoring. These networks expand attack surfaces that are hard to secure with traditional technologies.

SOLUTION

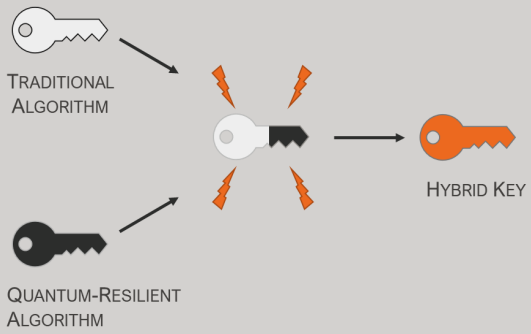
Patero solutions reduce attack surface and protect critical communication networks from today's advanced attacks and tomorrow's quantum-powered attacks. The solution was designed to work with existing assets without compromising performance, to avoid downtime and IT complexity.

Conclusion:

Creating resilience across critical infrastructure will depend on **safely** harnessing digital information. Patero solutions support a structured framework to upgrade security for sensitive data and critical operations.

Critical infrastructure is physical backbone of US National Critical Functions (NCF). NCFs, like utilities, pipelines, financial institutions and supply chains, can be defined as entities so vital to our everyday way of life that their disruption, corruption, or dysfunction would have a debilitating effect on national and economic security.

Technology adoption (e.g. sensors, cloud, IoT, AI) essential to digital management in NCFs has increased attack surfaces that threat actors can exploit. Specific examples include home offices, connected field workers, remote monitoring and multi-site communications. While these technologies have become essential to everyday operations, leaders in NCF now have to the weigh the advantages of digital transformation against the potential impact of cyber attacks.



Patero's future-safe security includes:

- Network and cryptographic risk assessment
- Cloaking or darkening endpoints and networks
- Hybrid cryptography
- Perfect forward secrecy
- Reduced attack surface

Data security depends on network integrity and cryptographic hygiene, especially when communications cross security and enterprise perimeters. Patero solutions help organizations reduce attack surface and secure communications across insecure networks now and over time.

PanoQoR™ - scans networks for security to identify faults and assess risks
EndoQoR™ - scans products, applications and devices to catalogue cryptographic libraries and assess risk
CryptoQoR™ (QoR) - crypto-agile, software-based hybrid cryptography solution to create protected communication channels that reduce attack surface and protect communications, even in remote or decentralized operations
Qorsight™ - centralized monitoring solution to maintain and update QoR-protected endpoints

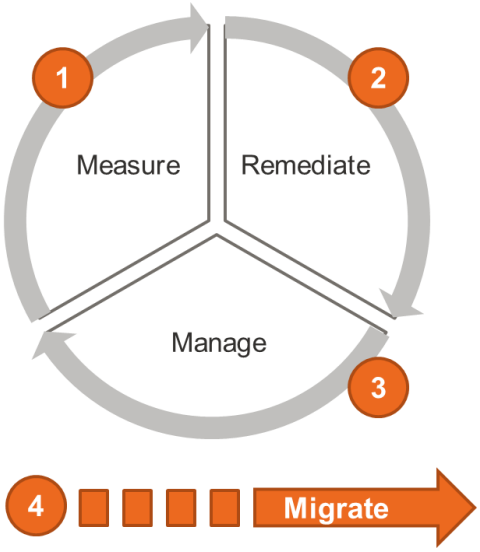
The Patero security suite can be used by enterprise security teams, consultants or security providers to structure security upgrades in critical infrastructure and operations.

PATERO
QUANTUM SECURE COMMUNICATION

Solution Approach

Executive Order 14028, National Security Memorandum 10 and the US National Security Strategy state that agencies, enterprises and corporations responsible for critical infrastructure modernize security to protect against current and future quantum-based cyberthreats.

Patero's future security suite includes solutions to help organizations assess and remediate security risks that expose them to man in the middle, harvest now/decrypt later and eavesdropping that compromise operational privacy, confidentiality, operational integrity and safety.



1. **Measure —** Networks and cryptographic libraries can be difficult to inventory, and organizations can be unaware of the breadth and scope of dependencies on public key infrastructure. PanoQoR and EndoQoR inventory and score both to help companies structure remediation and upgrade strategies.

2. **Remediate —** QoR is a software-based, hybrid post-quantum encryption solution. It works at the kernel level of Linux– and ARM-based operating systems and can be deployed in a broad range of compute environments including gateways, edge bare metal, and virtual cloud environments and microcontrollers to work with both existing and new infrastructure. QoR-enabled communications are protected by a series of cryptographic methodologies that help organization reduce attack surfaces, protect data in transit and over time, migrate to post-quantum encryption. The solution is also crypto-agile, which means that it can be updated as standards and technology evolve. QoR does not introduce significant latency or network overhead to work with operations sensitive to timing.

3. **Manage —** Qorsight is a centralized management plane to update and manage QoR-protected endpoints. Qorsight can include periodic scans to refresh network and cryptographic risk profiles.

4. **Migrate —** In the near term, Patero security solutions enable security leaders responsible for national critical functions to reduce attack surfaces, cloak critical assets and assess and remediate network and cryptographic vulnerabilities. Over time, Patero enables organizations to align cryptographic and security migration with business priorities and emerging standards.

Common use cases:

Enabling secure Edge-to-cloud connectivity, remote monitoring, OT-IT integration, operational privacy, classified or sensitive data transmission

Preventing Eavesdropping, harvest now/decrypt later, man-in-the-middle, tampering, spoofing and command and control attacks

To contact Patero, please visit:

www.patero.io

Organizations no longer have to compromise between security and digital capabilities. Instead, they can reduce attack surfaces and start upgrading security to align with principles guiding EO14028, NSM-10 and NIST PQC migration frameworks.

7757 Baltimore Ave.
Suite 1603
College Park, MD 20742
www.patero.io

PATERO
QUANTUM SECURE COMMUNICATION