

Quantum Private Networks

by Patero



- Quantum-safe, NIST post-quantum encryption
- Edge-to-anything quantum-safe tunneling
- Zero-trust endpoint cloaking architecture
- Software for low-touch, plug-n-play provisioning



A Quantum Private Network is a leap beyond traditional virtual private networks. QPNs deliver unique cloaking, security, and zero-touch deployment features that set them apart. QPNs are quantum-safe and crypto-agile.

Quantum Private Network (QPN) A NIST-compliant Solution for Critical Infrastructure



Emerging and Changing Security Needs

The shift to remote work has expanded the perimeter of corporate networks, increasing the complexity of securing access to enterprise resources.

Today, employees must connect to company resources from remote locations, often using

personal devices over unsecured networks. Ensuring secure remote access without compromising performance or user experience is a significant challenge. Moreover, the need for remote access extends beyond employees to include third-party vendors, contractors, and partners, further complicating the security landscape.

The security landscape continuously evolves, driven by new threats, technological advancements, and regulatory requirements. As remote work becomes more prevalent, organizations face the challenge of securing data flows between distributed networks of remote locations and corporate resources.

Traditional security measures designed for on-premises environments often need to be improved for the dynamic needs of remote offices. Businesses must adapt quickly to these changes, ensuring their security practices are agile and future-proof against current and emerging threats, **including those posed by quantum computing.**

The New Threat: Quantum

Quantum computing will bring unimaginable capabilities to science and business. No question. But they will also be used to crack the classical encryption we all use every day. In fact, the U.S. Government warns that adversaries are *already collecting our encrypted data because it will be decryptable later* with quantum computing.

Risks Can be Extraordinary

Legal offices, client financial services offices, trading offices, and many more can process millions or billions of transaction dollars. Keeping the details of these transactions out of reach of the bad guys - whether domestic thieves or international criminals – is a “must-do” for you and the sanctity of your clients.



Data Sensitivity can Stretch Decades

Yours or your client’s transactions are the sole of your business. Imagine how it might affect your business if the details of your transactions: who, what, how much, how long, and more were instantly discoverable by anyone with an itch to scratch. It’s well known that our foreign adversaries are snarfing up every data packet transiting the Internet. Why? Because in a few years, all that data will be decrypted with a quantum computer and stuffed into an AI engine.

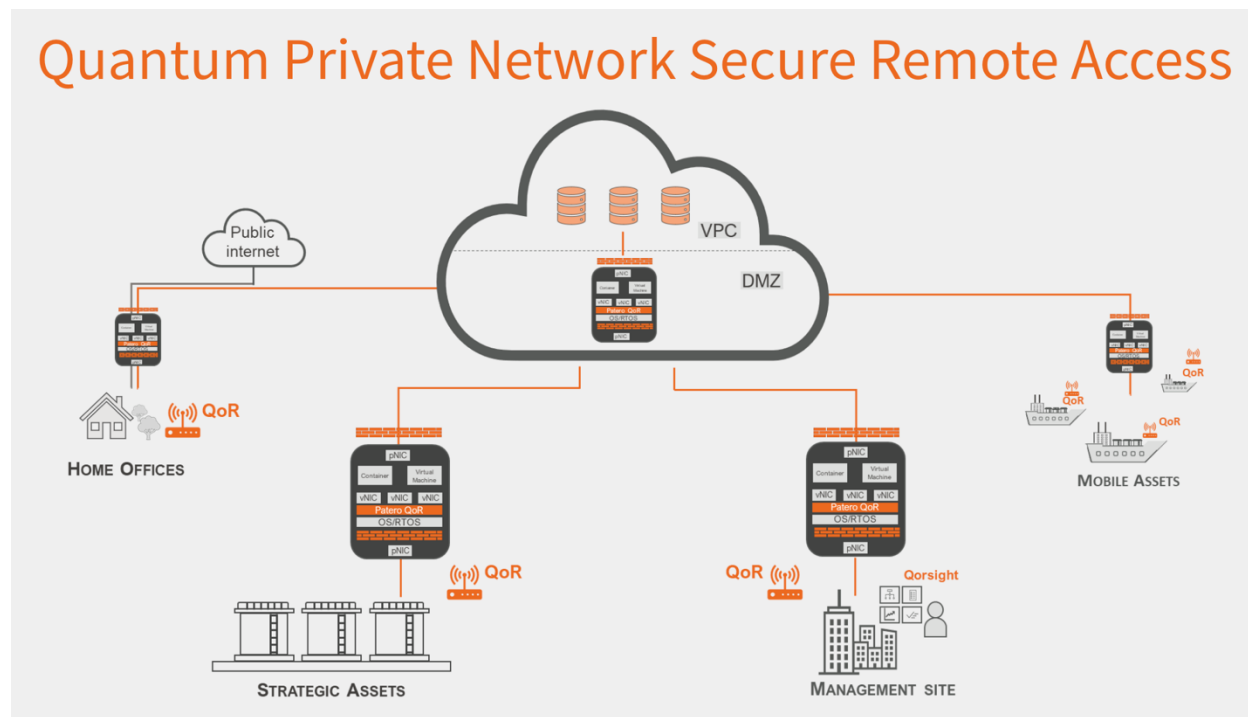
With that done, it’ll be as simple as asking: What were the terms of the contract between (your) company A and their supplier? What did client B pay for XYZ asset, and who witnessed the transaction?

ChatGPT is a toddler today. When today’s encrypted data is decrypted and made available to anyone with a penny and a motive, that toddler will be a terrible monster.

Quantum Safety from SNDL is Essential

That’s why quantum-safe encryption is so important *now*. The bad guys are storing our encrypted data now for decryption later (SNDL). Take it from Congress, the White House, the NSA, and NIST. The U.S. government is driving a national encryption upgrade. The NSA

has *already implemented quantum-safe encryption* for itself. With NIST's standardization of quantum-safe encryption, small and remote offices can protect their “today” data as it traverses the “vulnerable attack” surface of the Internet from attacks tomorrow.



Edge-to-Anything Quantum-Safe Data Channels

Secure data channels have been a persistent challenge for industries and critical infrastructure sectors. Cloud data historians, artificial intelligence (AI), machine learning (ML), and supervisory control and data acquisition (SCADA) systems are difficult to deploy because establishing and maintaining edge security infrastructure is tricky and requires maintenance. As a result, it becomes challenging for operational technology (OT) data to pass on its way to the cloud.

- Typically, system integrators need to work with organizational OT and information technology (IT) resources to install hardware and configure layers of network firewalls to establish secure data outflow. However, it is common for IT/OT teams to mistakenly misconfigure these systems, leading to data blockages and rendering critical cloud-based services unavailable.
- QPN requires only a single outbound port and typically no OT/IT configuration. The QPN soft gateway (or device gateway) must only be powered on. It will immediately connect to its known private QPN cloud virtual gateway, exchange identity, and then

auto-negotiate and generate hybrid-PQC session encryption keys.

- The best part is that a system integrator is not required, saving time and money for the application service provider. Additionally, the network administrative load on OT/IT and CSO staff is reduced or eliminated.

Some businesses must keep their data, email, applications, and communications to themselves. They cannot take the risks that come with cloud service providers (CSP), or they have clients who don't want their data hosted in shared CSP application environments.

The Benefits of Using a Private Data Center

- Customizable to your precise needs
- Total control and oversight
- No resources shared with other businesses

Quantum-safe Secure Remote Access

Accessing OT/IT systems to implement and manage configurations, updates, or patches must be done either on-premises by the vendor or system integrator (SI) support personnel or by enterprise OT/IT resources. On-premises access is costly, burdens corporate personnel hosting vendors/SIs, and unnecessarily broadly exposes enterprise network resources.

- QPN zero trust network access (ZTNA) places cloud and enterprise network elements on the same local IP address range. Cloud applications can, therefore, appear to reside on the local enterprise IT/OT network. Temporary virtual network terminals can be created as remote access points to local enterprise hosts.
- A QPN can spawn a virtual cloud-based jump host providing ephemeral access to local host/served applications from remote endpoints — all over quantum-safe, hybrid PQC channels.

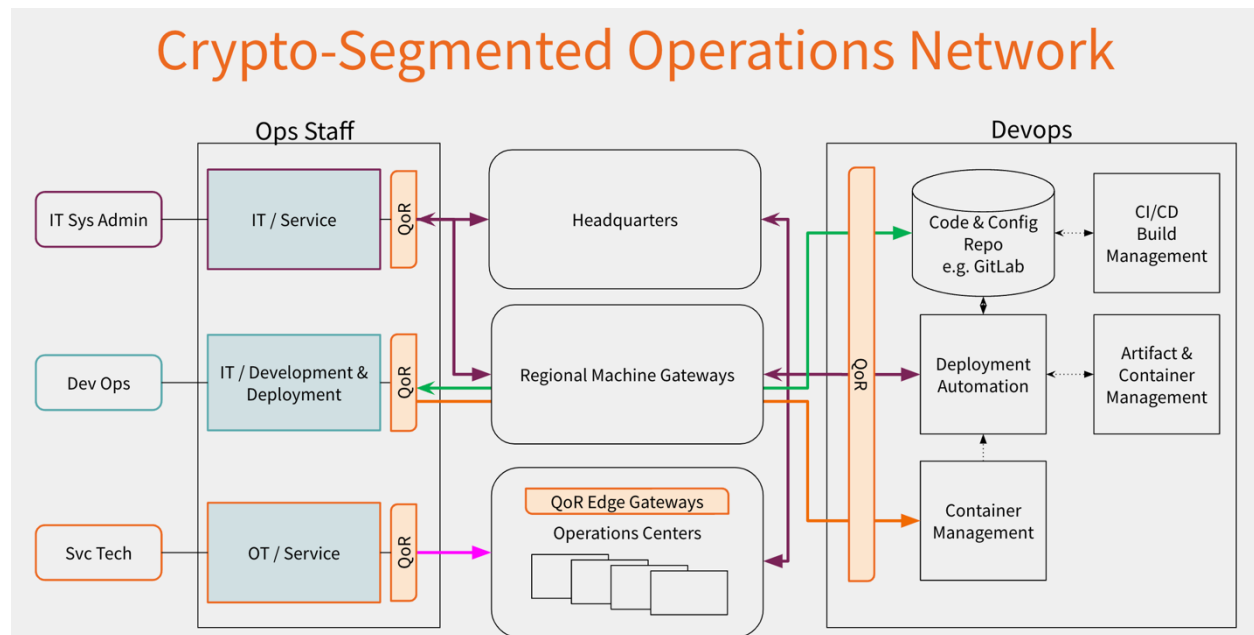
Zero-touch, Edge AI/ML Deployment

Edge computing is growing at a >32% CAGR. Deploying edge computing devices typically requires the engagement of SIs, OT/IT resources, truck rolls, and the configuration of often expensive firewall systems.

- Deployment of edge AI, edge ML, or distributed intelligent edge computing can be time-consuming and expensive. The ideal deployment model would be zero-touch plug-and-play. Solution providers would ship pre-configured edge computing devices that require only power and a network connection. The device would reach the service provider's quantum-safe virtual cloud gateway through the enterprise firewall and auto-establish a secure data channel without requiring OT/IT configuration.

- Patero PQN solutions are software that includes the Patero CryptoQoR crypto-module, Qorsight management, and configuration server. CryptoQoR is easily configured to call a Qorsight configuration server using a quantum-safe encrypted channel for instruction. The CryptoQoR-enabled edge endpoint then drops its configuration connection and requests a connection to the service provider's quantum-safe cloud virtual gateway.

The cloud gateway service, presented with the edge gateway's public pre-shared quantum certificate, accepts the connection request, negotiates a hybrid PQC session key, and secures the edge-to-cloud channel with no administrative *intervention needed*.



Segmented Industrial Operations Network

Network segmentation increases security posture and reduces attack vectors. In critical infrastructure - whether hamburger "manufacturing" robots or machines stamping parts – network segmentation with secure remote access is the optimal operational solution.

- A food manufacturing robot will have a local control OT network but a cloud-based manufacturing execution system or knowledge (recipe) management system. The enterprise will also have a separate maintenance operation system collecting machine data at the edge for insight generation in the cloud. Finally, a retail enterprise network will have a cloud financial transaction and tracking solution fed by on-premises payment systems. Finally, there exists across these three segments the need for temporary access by employees and vendor service technicians for support and maintenance.

- Segmenting each network by function and again by location (e.g., regional data centers) is a daunting task - especially for operations that do not or cannot employ full-time IT resources. For organizations that do not have on-premises IT support or their own mobile IT infrastructure, maintaining a complex set of segmented networks is nearly impossible.

QPN Attributes:

- Software cryptomodule
- Supports most modern Linux distributions
- An IP Layer 3 solution supporting IPv4 and IPv6
- Edge and cloud quantum encrypted channels
- Protocol compatible: wraps existing protocols in post-quantum cryptographic (PQC) channels
- Frustrates unwanted packet inspection
- Secures data from observation when transiting compromised network elements
- Thwarts steal now, decrypt later attacks
- Closes IP endpoint ports from response-seeking adversaries
- Zero-touch, NAT traversing, deployment
- Hybrid or strict PQC session keys
- Crypto agile - user-selectable encryption algorithms and on-the-fly algorithm upgrades
- Zero trust network architecture using “Quantum Certificates” for endpoint authentication
- Nimble architecture solution:
 - Remote access
 - Site-to-site
 - Mobile app remote access
 - OEM QPN (mobile app, µC, embedded NIC)

Patero Ecosystem Partners



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

