Ultra Secure, Quantum-Safe, Private Data Center with Patero Quantum Private Network

- **Quantum-safe, NIST standard encrypted tunnels**
- **Cryptographic network segmentation**
- **Cloaks endpoints and secures data with zero trust**
- **Zero-touch, plug-n-play provisioning**

PATERO
QUANTUM SECURE COMMUNICATIONS

Some Businesses Need a “More Private Solution"

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.

A few decades ago, when employees were all within enterprise walls, this kind of privacy was easily managed by the enterprise.

But running a modern enterprise “data center” is no easy matter, and it is better to be outsourced.

That doesn’t mean handing over your and your clients’ data to a commercial cloud service provider. Private data centers provide “bare metal” hosting services, allowing business to run their own email, storage, applications, and communications servers without concern over the hosting provider also being the company application provider.

© École polytechnique - J.Barand

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 soul 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.

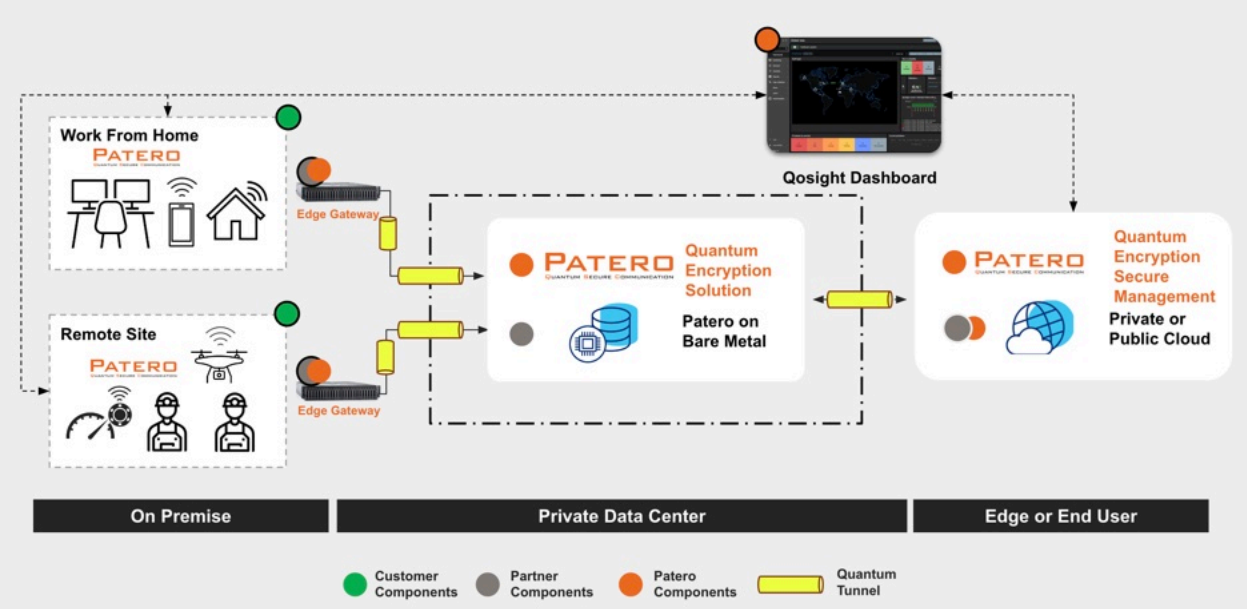
Quantum Private Data Center

A quantum private data center (QPDC) secures your data from SNDL attacks, keeps it quantum-safe into the future, and provides all the privacy benefits of a private data center.

The Benefits of Using a Private Data Center

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

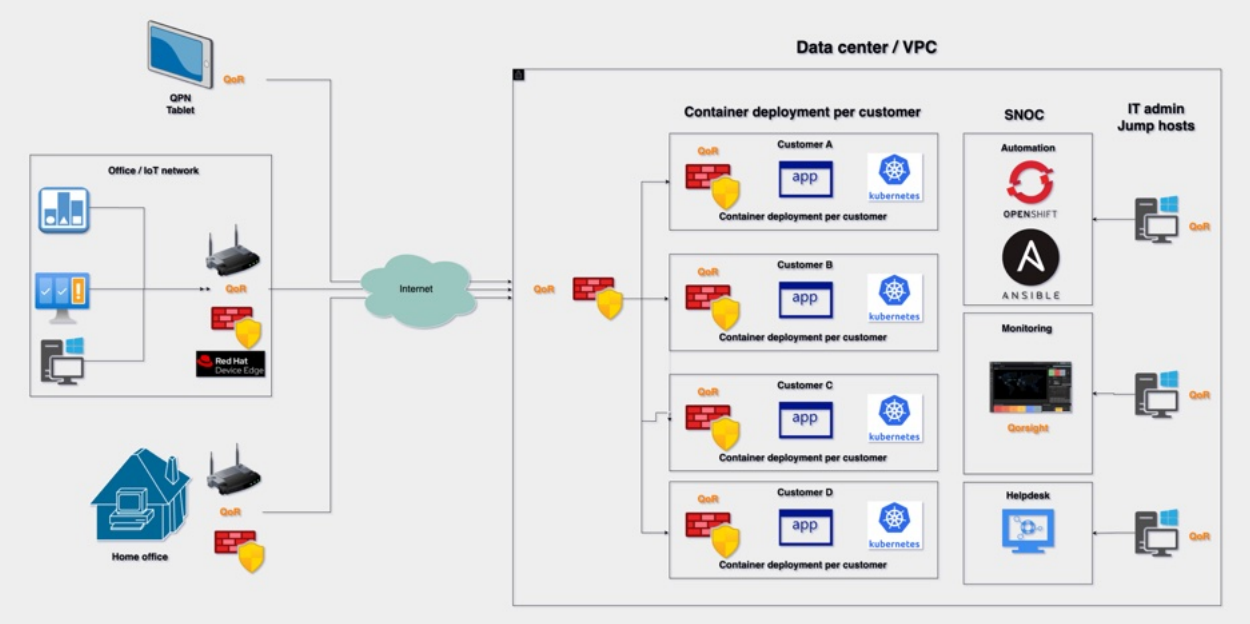
Patero quantum private network solution paired with private data centers delivers a QPDC – a data and application hosting environment you control and oversee. All data flows into and out of the QPDC are encrypted with post-quantum cryptography. Those network endpoints that must be reachable via the Internet can be "cloaked" from discovery by malicious actors.



Features of a Patero Quantum Private Network

No IT Resources to Administer Devices

Organizations needing private cloud networks may not have insufficient IT resources to go it alone. To make matters more challenging, they often rely on “bring your own device” (BYOD) strategies. Choosing, installing, and maintaining specialty security applications such as VPN clients becomes overwhelming – creating additional security and operational problems. When team members upgrade BYOD laptops, the cycle of installing, updating, and maintaining starts again – for the “designated IT person.” Add the “quantum-safe” requirement, and a substantial challenge emerges. That’s where Quantum Safe Remote Edge-to-Anything gateway strategies come into play with quantum private networks. BYOD devices need only connect to the premises gateway, guaranteeing sensitive data is encrypted with quantum-safe protocols.



Multi-Tenant, Quantum Private Data Center

Zero Trust Architecture is a Must

Zero trust means that hybrid-cloud resources must be inherently untrusting of remote premises networks and, by default, assume no entity, internal or external, can be trusted. ZTA requires strict verification of all access requests and continuous network traffic monitoring. Patero’s quantum private networking solution cloaks Internet-facing endpoints from unauthorized connection requests. Patero only responds to connection and authentication requests from trusted remote network resources. This approach is vital for safeguarding remote offices against sophisticated threats, including those posed by quantum computing.

Defense in Depth and Zero Trust Architectural Layers

In the face of increasing security threats, adopting a defense-in-depth strategy combined with ZTA is essential. Defense in depth involves implementing multiple layers of security controls across the network, ensuring that even if one layer is breached, others remain intact to prevent compromise. Quantum encryption is one layer, and zero trust authentication is another. Further implementation of user identity and access management with application access controls is supported through Patero quantum private network tunnels.

Crypto-Agile and Quantum-Safe

After eight years of rigorous algorithm testing, NIST standardized only four of ninety-two candidate algorithms to secure data against quantum computer-powered cyber-attacks. It's unknown how long the selected algorithms will stand up to advances in artificial intelligence-driven hybrid classical-quantum computer algorithms being developed by nation-states and hyper-funded espionage rings. So, quantum private networks must be secured with "crypto-agile" solutions capable of cryptographic algorithm updates and upgrades without redeployment of capital equipment or suspending operations.

Remote Device Management

Remote premises rarely have on-site IT resources. Support, therefore, typically requires truck rolls for connected networking device management. The total cost of remote premises network management can be significantly reduced when a quantum private network is employed. QPNs allow the administration of premises equipment remotely via quantum-secure private network tunnels, saving travel time, minimizing lost productivity, and reducing insured driver costs.

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