Aliro™

Quantum Networks for Secure Data Center Connectivity

Aliro

www.alirotech.com

Quantum Networks for Secure Data Center Connectivity

Summary

As quantum threats escalate, securing high-risk data center links demands a layered approach combining PQC, QKD, and QSC to protect the sensitive data underpinning enterprise and national infrastructure.

Introduction

Replacing today's encryption methods is increasingly urgent as we face security threats from advanced AI, quantum computing, and other sophisticated attacks. Data center-to-data center links are critical to enterprise and national infrastructure, and they are especially vulnerable to interception, man-in-the-middle, and Harvest Now Decrypt Later (HDNL) attacks. These links often carry a high volume of highly sensitive data, making them primary targets for nation-states and cybercriminals.

Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Secure Communications (QSC) can be layered for efficient and effective quantum-resistant protection against these threats.

Who Needs Quantum Security Most?

The fiber optic cables that serve as the backbone of our global connectivity are vulnerable to interception, to man-in-the-middle attacks, and to Harvest Now Decrypt Later (HDNL) attacks where encrypted data is quietly harvested with the intent to crack it later using quantum computing. These tactics are not theoretical threats; they're happening today.

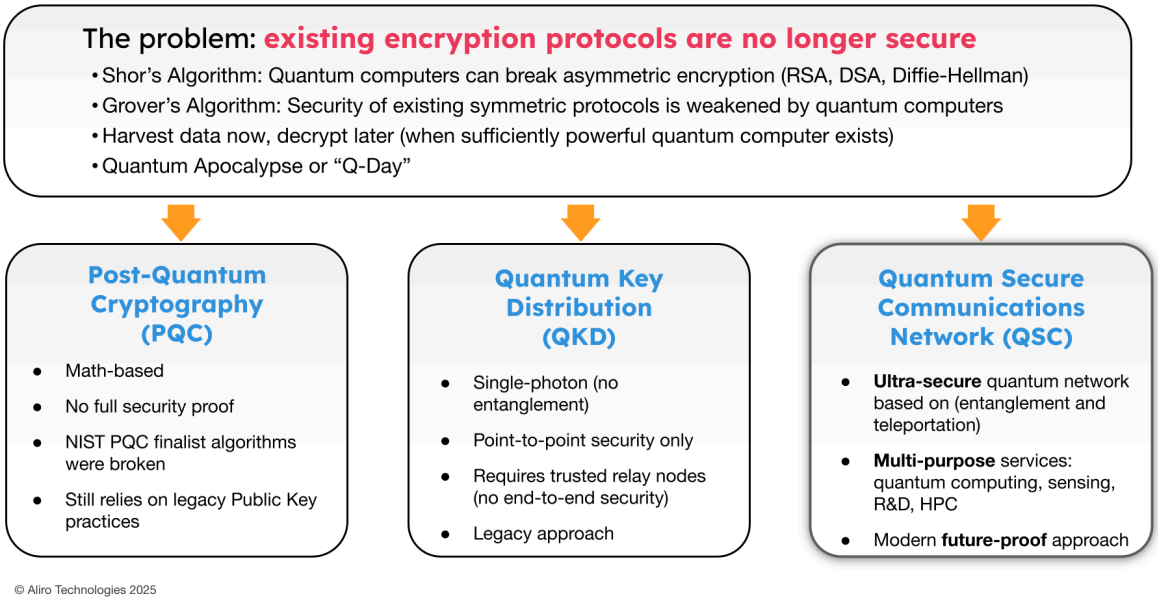
Adversaries, bad actors, and even nation states are focused on the most lucrative targets: those links that carry the highest volume and most data-rich communications such as financial hubs, healthcare systems, pharmaceutical IP vaults, energy grids, and sovereign infrastructure. This is not an abstract threat. A breach between a Fortune 100 company's HQ and its cloud could yield a treasure trove of sensitive data. A compromised disaster recovery link could paralyze operations in the midst of a crisis.

Quantum Secure Communications is a mission-critical solution for the world's essential sectors. Financial institutions underpin national and global economies, making them prime targets. Healthcare systems and pharmaceutical companies hold vast stores of sensitive data and IP, and our society's health depends on their resilience. Governments and entire countries are moving to harden their digital infrastructure to protect national security interests. The energy sector and infrastructure such as water distribution rely on secure, uninterrupted

communication. In short: if your operations are foundational to modern life, quantum-powered security is not optional, it's the best mechanism for securing these vulnerable connections.

A Quantum-powered Strategy for Data Center Connectivity

Today's infrastructure must defend against both immediate and looming threats. There are a number of different methodologies and technologies for securing our network infrastructure.



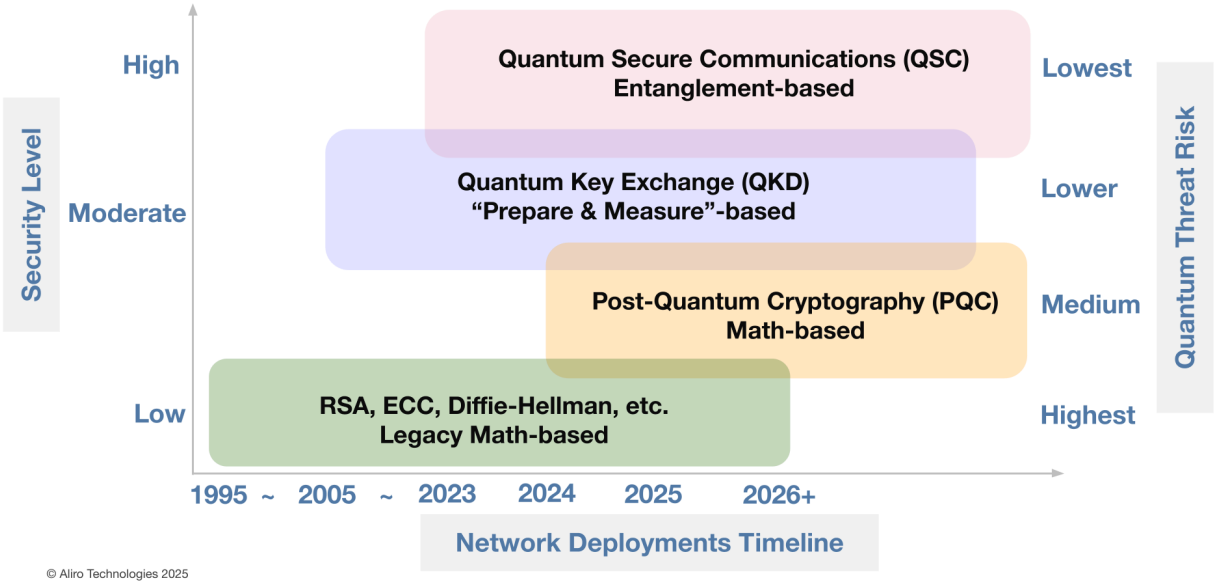
Post Quantum Cryptography (PQC). PQC is a well known methodology today. PQC consists of math-based algorithms that replace the legacy math-based algorithms that are used within asymmetrical and symmetrical encryption. While not provably immune to future attacks, PQC significantly improves upon legacy algorithms such as RSA. The National Institute of Standards and Technology (NIST) has selected a set of candidate standards following rigorous public testing. Several early contenders failed, with some unable to withstand basic decryption attacks using conventional laptops. Three strong finalists are now available for implementation. NIST is working to release more PQC standards in the near future. PQC will become a pervasive tactic for protecting data.

Quantum Key Distribution (QKD). QKD advances security by leveraging quantum physics to establish shared keys. Using single encoded photons, also known as qubits, QKD creates encryption keys that are more secure than those generated by classical methods. This is a prepare-and-measure, point-to-point security mechanism and requires trusted relay points to extend the distance of the links. There is no entanglement used in this approach.

Quantum Secure Communications (QSC). QSC is the gold standard, ultra-secure quantum network methodology that leverages entanglement and teleportation. This is the most secure implementation for protecting the high-volume links that carry the most sensitive data. QSC is modern and future-proof, and because it's entanglement-based this technology can carry out other applications such as interconnecting quantum computers, connecting distributed quantum sensors with one another, and other applications that we're not even aware of today.

Secure Networking Technology Landscape

Organizations must rethink how to secure their most critical communications. How do these methods compare in the secure networking landscape?



Looking back 30 - 40 years ago, RSA, ECC, Diffie-Hellman, and other math-based algorithms were the primary mechanism for securing and encrypting information across both public and private networks. Many times these algorithms were used over Multi Protocol Label Switching (MPLS) networks to provide a layer of encryption. Communications over dark fiber optic cables can be encrypted using these legacy algorithms. The challenge in using these algorithms is that they are being sunsetted because they are at-risk from quantum computers, supercomputers and even advanced AI as it becomes more sophisticated. RSA-based technology offers a very low security level right now, and the quantum threat risk is very high. It's the highest of all of the methods shown here.

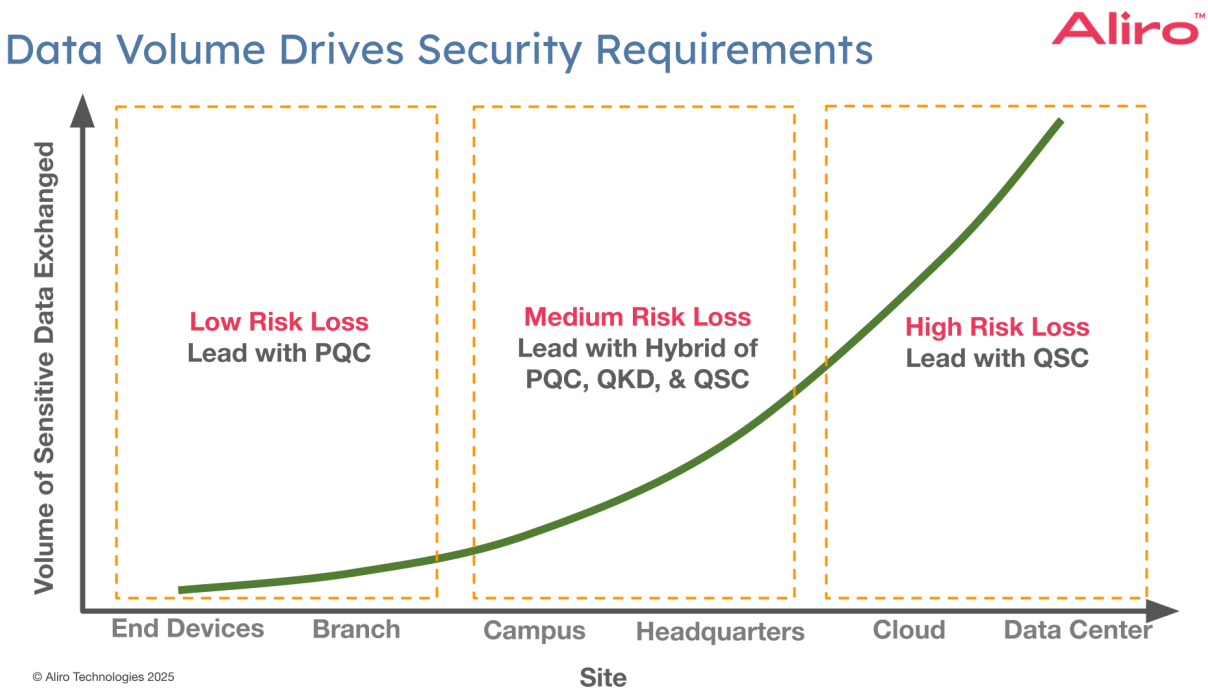
The next stage in the landscape is Post Quantum Cryptography (PQC). PQC offers increased security because it uses, for example, lattice-based methodologies that are more difficult for quantum computers to decrypt. We can't prove whether PQC will be resilient against advanced quantum computers. However, PQC has undergone a lot of scrutiny and been deemed a safe methodology to use for security. It is better at protecting data from advanced threats than RSA is.

The stage beyond PQC is Quantum Key Distribution (QKD). In the landscape of secure networking methodologies, this offers better than moderate security. QKD does rely on trusted relay points, which are points where data is decrypted and re-encrypted, creating a vulnerability at each relay. Every trusted relay point represents a gap where information and keys are exposed. This vulnerability makes this a moderate security solution and is a better option than PQC in many cases.

The highest security level that can be achieved is through Quantum Secure Communications (QSC). This technology is based on quantum mechanics and uses the property of entanglement, where photons are entangled with one another. These entangled photons are distributed across the network, and those entangled photons are then used to create shared keys and secrets at end nodes without using a public exchange. This method has the lowest quantum threat risk possible.

Efficient and Effective Quantum-safe Security

In a quantum-enabled world, not all links in an enterprise network are equally impacted when it comes to securing data. The volume and sensitivity of data exchanged across different segments of an organization should directly inform which quantum-safe security technologies are deployed. Modern infrastructure demands a tiered, risk-based approach to protection that starts with Post-Quantum Cryptography (PQC) and scales up to Quantum Secure Communications (QSC) as risk and data volumes increase.



At the outer edges of the enterprise are endpoints like smartphones, laptops, and tablets, where data exchanges are relatively lightweight. While these devices do communicate with clouds and data centers, the volume and criticality of the data they handle are comparatively low. In these scenarios, PQC offers sufficient protection. It replaces legacy encryption schemes like RSA and ECC with quantum-resistant alternatives, and it should be considered the new default, base-line layer of encryption across the enterprise.

Branch offices and remote sites represent a step up in the scale and criticality of data, and a step up in risk. These locations may host dozens to hundreds of employees, each engaging in daily operations that generate sensitive client, logistics, or financial data. The volume of information justifies the continued use of PQC, offering a reasonable balance between protection and implementation effort for these mid-tier environments.

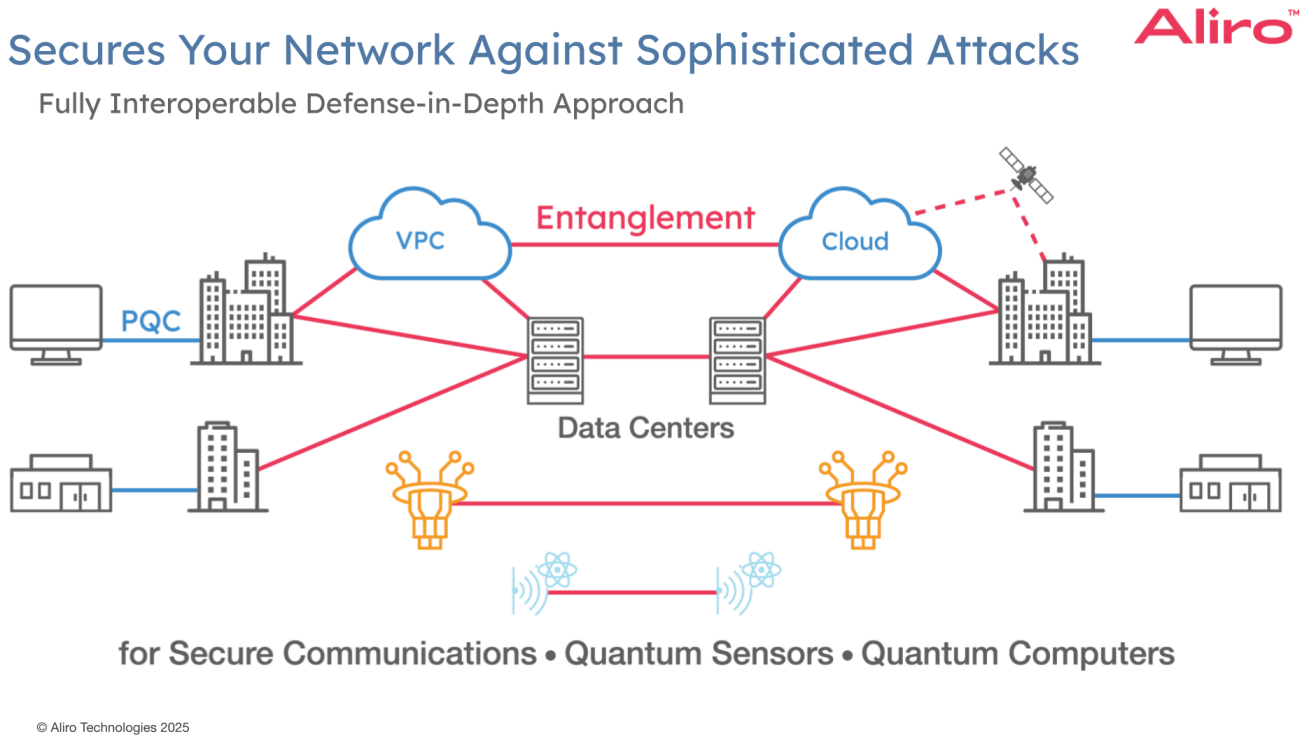
As the infrastructure scales to larger, more centralized environments such as corporate campuses or global headquarters, the density and sensitivity of data dramatically increases. These sites typically handle critical financial records, personal identifiable information, and proprietary business data. In these medium-risk zones, a hybrid strategy is warranted. PQC remains the baseline, but organizations should augment it with QKD where feasible, and begin integrating QSC wherever possible.

At the core of an enterprise are the highest-risk assets: cloud connections and data centers hosting workloads, data resources, and databases. Private, co-located, and hybrid cloud

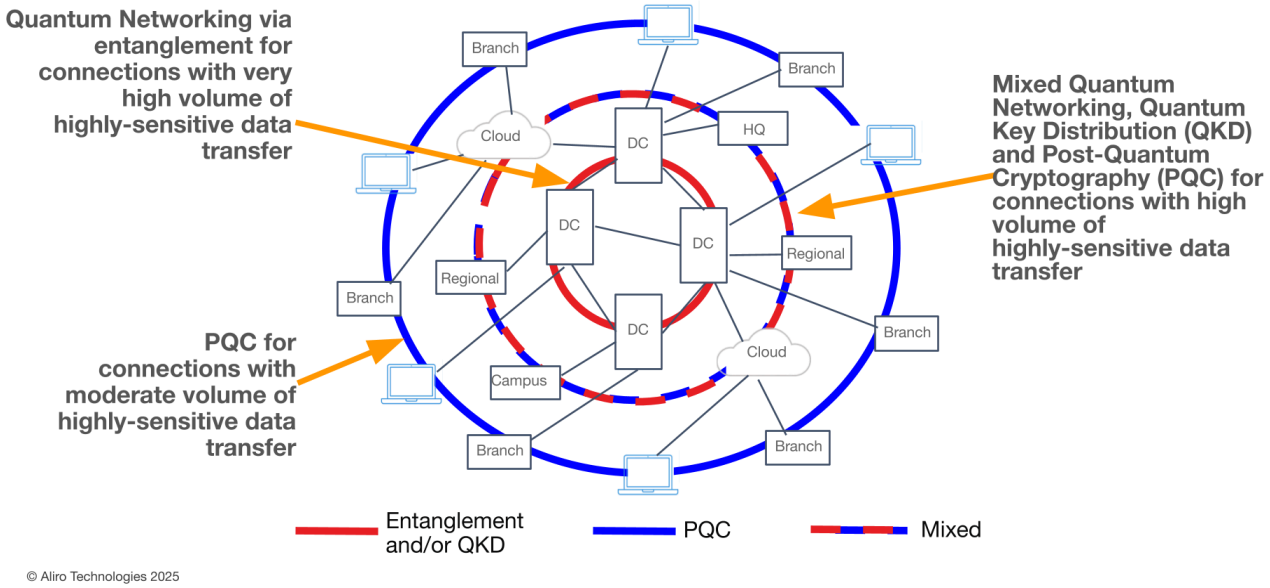
environments are all areas of the network that carry massive volumes of high-value, highly sensitive data. This is where the risk of quantum-enabled breaches is greatest, and where the strongest defenses are necessary. QSC should be the main security methodology for these areas.

Mapping the Modern Secure Network Architecture

Enterprise and public sector networks often span a variety of interconnected environments ranging from endpoints and branch offices to regional hubs, campuses, headquarters, cloud infrastructure, and mission-critical data centers. This architectural sprawl creates a dynamic threat surface that requires layered security.



Adopting a concentric, defense-in-depth model addresses this complexity by implementing an increasing level of security as the volume and sensitivity of the data increases. An example of this mode is shown below, with red lines indicating entanglement-based security and blue lines indicating PQC security measures.

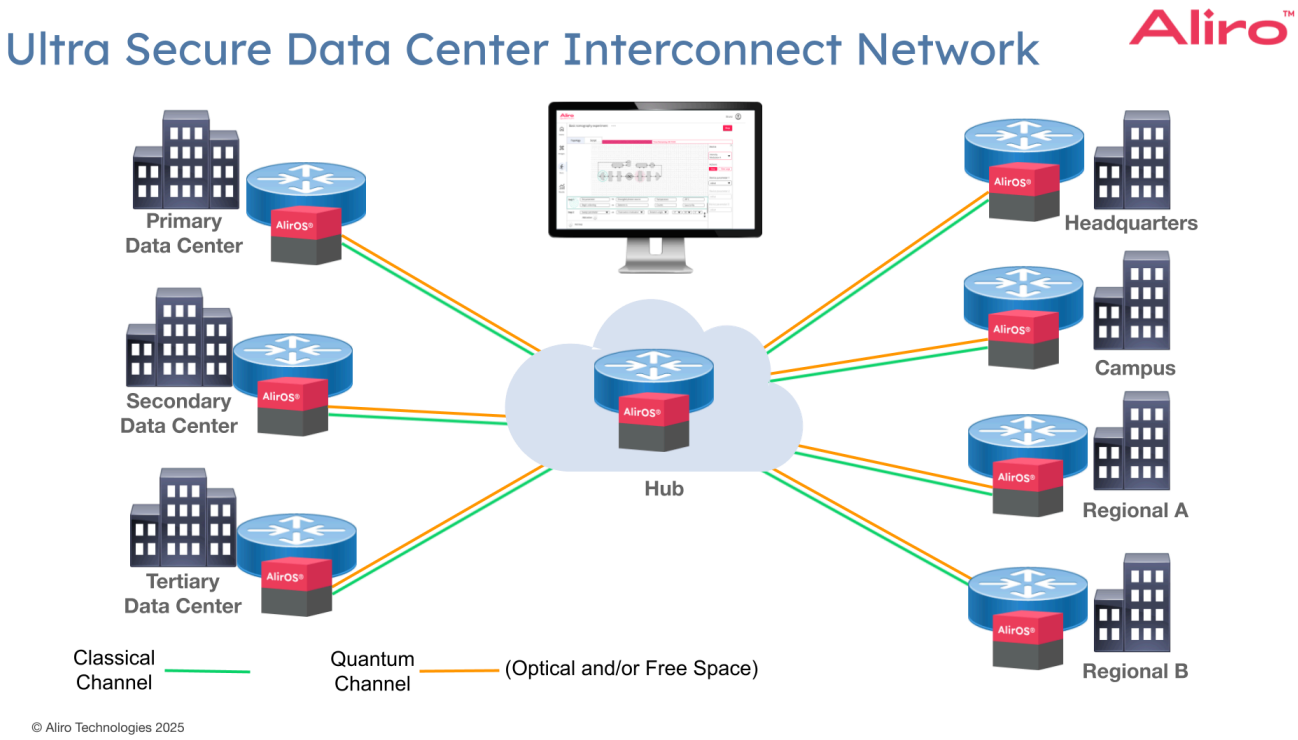


At the outermost edges, PQC provides foundational protection. PQC is deployable across branch offices and endpoint devices, offering a practical defense against harvest-now-decrypt-later attacks.

The mid-tier, at campuses and headquarters, a hybrid approach becomes essential. Here, PQC is augmented with QKD and QSC.

At the core, data center-to-data center and data center-to-cloud connections are the highest risk zones. These links are protected by entanglement-based QSC.

Zooming in on the core links, a common network for data center interconnect is a hub and spoke model. The topologies for quantum networking often mirror the topology that is already in place today for a classical network. Any topology used for classical networks can be used with the quantum dimension of the network. In the example below, a central hub node serves as the source for entangled photons, distributing them to primary, secondary, and tertiary data centers on the left as well as to major sites like headquarters and regional centers on the right.



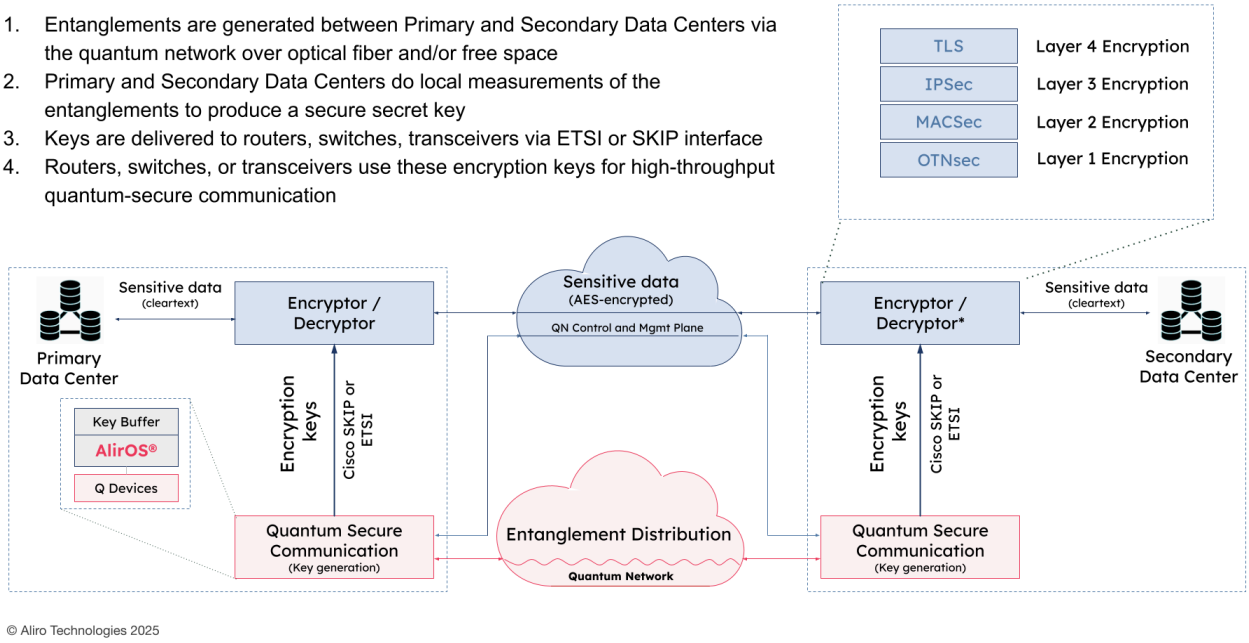
These sites could be geographically dispersed and could have various roles, such as disaster recovery. Any one of these sites could be co-located facilities that are being used as data centers. These sites could also be clouds from any one of the major cloud providers: AWS, Azure, Google, Oracle, etc. To the right are connections to a headquarters, campus, and a couple of regional locations. All of these are connected to a hub, and that hub is where the technology for entanglement generation is housed. Entanglement will be generated at that hub, and entangled photonic qubits will be distributed to the sites. This entanglement can be between the hub and the location, as shown, or it can be between any two sites that are connected to one another directly.

Each site is connected with a classical channel and a quantum channel. The quantum channel could be through optical fiber or it could be a free space connection. The quantum channel carries the unique information delivered via qubits and conveyed on either end of the network through entanglement in order to provide secure keys and potentially other communications.

It's important to note that all the classical infrastructure deployed today could be preserved and there is a high likelihood that no changes to that infrastructure will be required. This secure data center interconnect can be deployed with existing classical infrastructure and the quantum channel is integrated into this existing infrastructure.

Quantum Network Integration Details

Quantum infrastructure marries with the existing classical infrastructure as shown below.



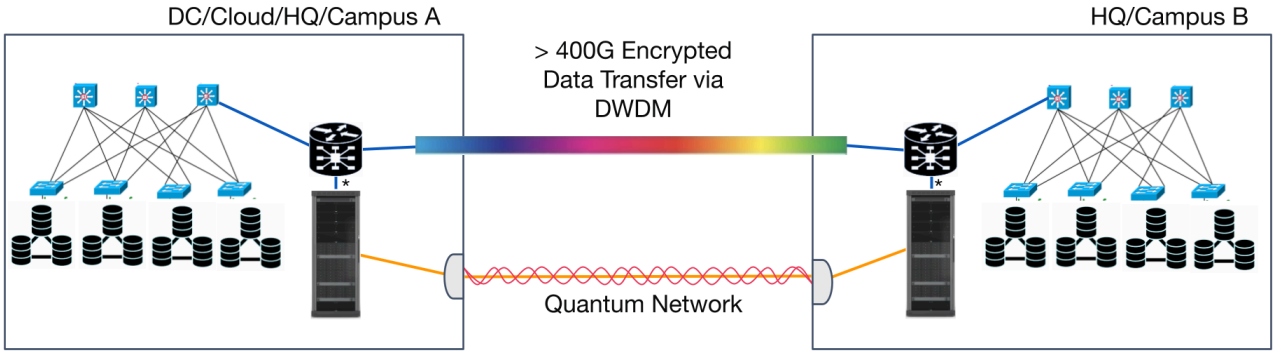
In this example, the primary data center on the left is connected to another location on the right. This could be a headquarters or a campus location – it doesn't matter what the location is, what the site is, and what the make up of that site is. Entanglement is generated between the primary data center and the secondary data center via the quantum network.

The quantum network is shown in pink and above it in blue is the classical network, the network that is currently used. That network today is very likely running three out of four of the encryption methodologies noted in the box in top right: TLS, IPsec, MACsec, and OTNsec. Any one of these in use today or in the future in that classical network is preserved and maintained. The network continues to use that methodology. The difference is that key material is no longer exchanged via public-key cryptography, eliminating a major vulnerability exploited by quantum computing. In other words, asymmetrical key exchange, such as what normally occurs with RSA to establish the secrets on either end, is no longer used. There are no public keys exchanged. What happens instead occurs through entanglement-based QSC. Keys are generated through entanglement, delivered securely via the quantum channel, and injected directly into existing encryptor/decryptor systems using standardized interfaces. Between the locations is a complete encrypted channel using symmetrical encryption, such as AES 256 or AES 512, and the keys used to establish that secure connection are provided by the quantum infrastructure and no longer derived through a public key exchange. If there's

any attempt to read, copy, monitor, intercept or perform a man-in-the-middle attack on the quantum channel, it is immediately detected and there is a notification to stop generating keys on that channel and use another backup mechanism or to use a store of keys that have already been buffered. Many times these stores of keys can last for months without re-establishing a new key on the quantum channel.

QSC Between Data Centers, Headquarters, Campus, and Clouds

Using the example below, we can take a deeper dive into the interconnection between two sites. On the left could be the primary data center, and to the right could be the headquarters or campus location.



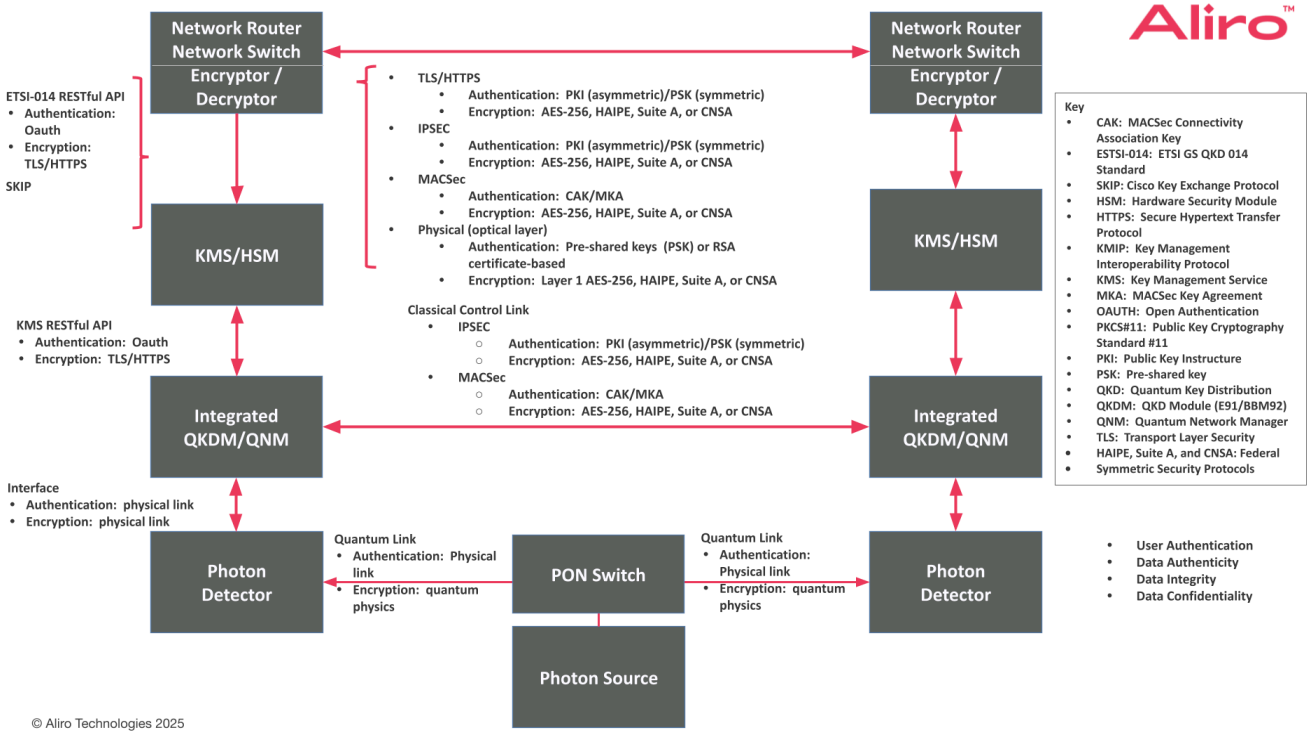
The example shows modern leaf-spine networks. Workloads, applications, storage databases are all running and connected to all the switches within the data center. Other services are running there as well. The infrastructure on either side of the interconnect is preserved.

At each site, a compact rack-based deployment handles quantum key generation and orchestration and is connected to a dense wave division multiplexing channel that is likely part of the same router or switch that is used today in the existing infrastructure, likely running hundreds gigabits per second of encrypted data between those sites. This infrastructure can be preserved as long as there is no active switching, no active components in the router or switch. Integration is streamlined via well-established standards, such as Cisco's SKIP protocol or ETSI 014, which define the interfaces between the quantum key sources and encryption hardware. This means the keys generated through entanglement or quantum key distribution can be injected directly into existing routers, switches, or transceivers with no need for a public key infrastructure.

Alternatively, a dedicated fiber strand can be reserved exclusively for quantum networking. This ends up being a turnkey model where the keys are generated, orchestration occurs, and services are integrated.

The Quantum-safe Stack

Understanding how quantum technologies integrate into existing infrastructure is essential. What changes, what stays the same, and where does the quantum layer actually live? Let's take a deeper dive into the network stack, from traditional encryption at the top to quantum entanglement at the foundation.



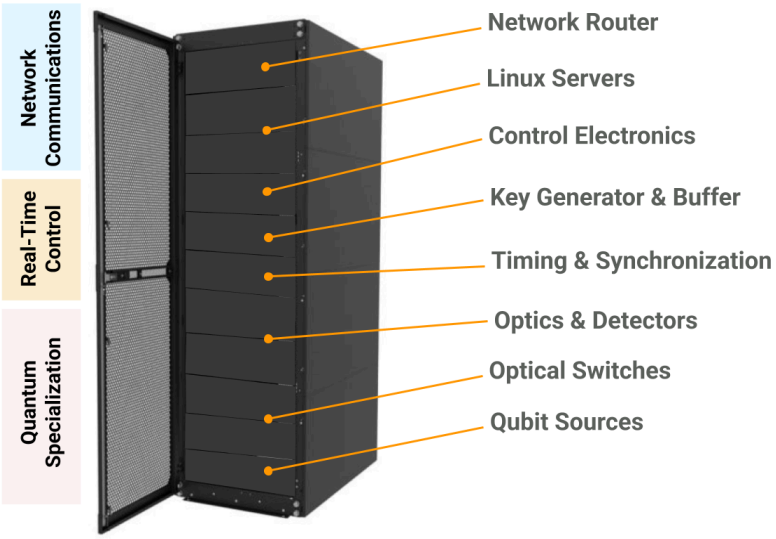
In the protocols mapped \ above, at the very top are the network routers and network switches. The encryptors / decryptors are there also. Most often in today's modern networking technology, those services are all integrated into a single device.
What is shown here is all of the encryption that occurs between those devices: IPsec, MACsec, symmetric encryption protocols like AES-256, Suite A, or CNSA. This part of the stack doesn't need to change. The critical shift is in how encryption keys are delivered. Traditional key exchange mechanisms rely on public-key cryptography, which is fundamentally vulnerable to quantum attacks. In a quantum-secure architecture, public key exchange is eliminated. The keys themselves are no longer transmitted at all, they are delivered via entangled photonic qubits.

Below the network router / encryptor / decryptor are the Key Management Systems (KMS) and Hardware Security Modules (HSM) that manage encryption keys and policies. These systems are enhanced to interface directly with quantum key sources via well-established APIs such as ETSI 014 and the Cisco SKIP Protocol. Below the KMS / HSM are integrated quantum key distribution modules. This is likely to be a BBM92 device for QSC operations or a BB84 device for QKD operations. The connection between the KMS / HSM and the integrated QKDM / QNM uses RESTful APIs, and the connection between them is a classical control channel.

At the bottom, the quantum channel is shown. There are photon detectors in each location, with a photon source that might be at a hub location. The photon source could be co-located within one of these facilities where it's providing and generating the entangled photons, but in this example it is located elsewhere at a central hub between locations.

The Quantum Data Center Rack

The physical rack deployed for Quantum Secure Communications in a data center might look surprisingly familiar, and it can be highly adaptable depending on the data center environment.



At the top of the rack, is a network router or switch, often the same models already used in the current network architecture. These may be co-located in the quantum rack or remain in adjacent racks, especially in brownfield deployments where existing infrastructure is being upgraded. Inside the rack are Linux-based servers handling orchestration, control software,

and key management services. These can also be located in separate racks if needed, or co-located in the same rack in the case of a green field deployment. There are the optics and the detectors inside the rack as well as one or two passive optical switches, depending on the network topology. Qubit sources could be here also, or located at a central hub.

Extending the Distance of Secure Links

One frequently asked question about quantum networks is how to extend secure communication across longer distances. Whether connecting geographically distributed data centers or securing intercontinental links between headquarters and regional campuses, the goal remains the same: enable end-to-end quantum-secure communications without sacrificing fidelity, latency, or interoperability. There are currently three primary strategies for extending the range of quantum-secure links:

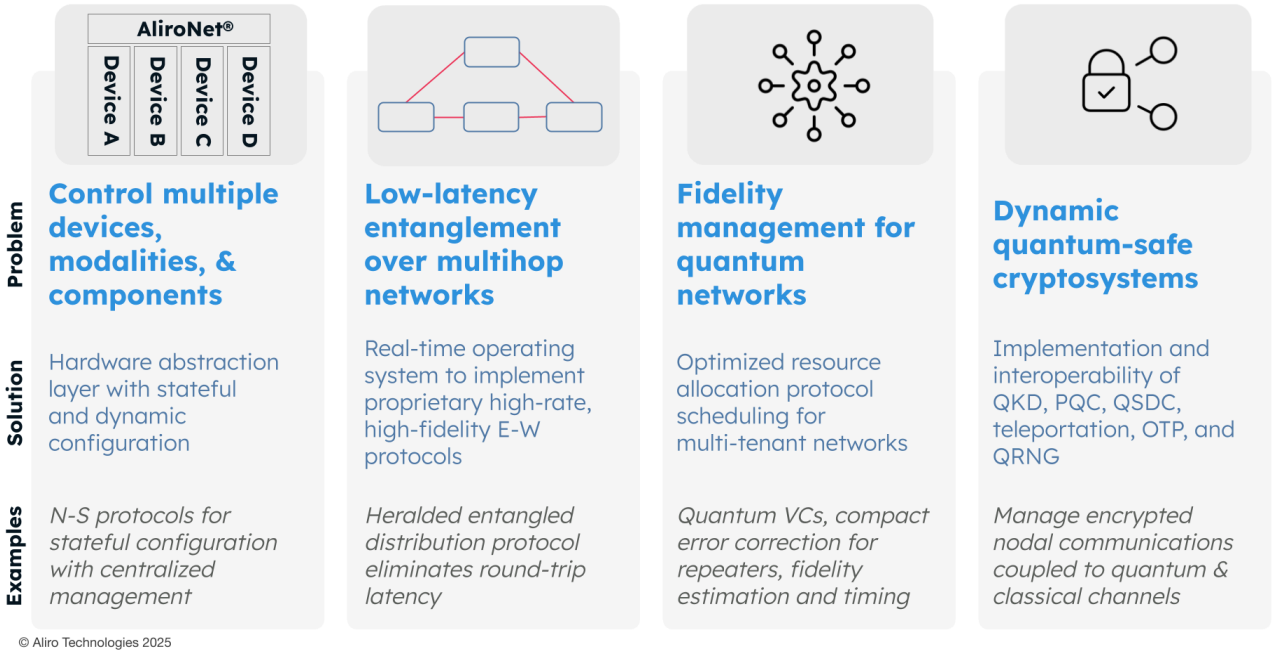
Free-Space Quantum Links via Satellites. Both QKD and QSC can take advantage of free-space links to extend the distance between nodes.

Trusted Relay Nodes. This approach can be used with QKD only. Each relay acts as a prepare-and-measure station. While effective, these relay points are security-sensitive because each relay introduces a point of exposure where encryption keys are regenerated and temporarily vulnerable.

Quantum Repeaters. This approach can be used with QSC only. A more advanced and secure alternative, quantum repeaters preserve quantum entanglement across longer distances via a process known as entanglement swapping. These devices use Bell State Measurements and quantum memories to extend entangled links without exposing key material.

Solutions to Operational Challenges of Quantum Networks

Several technical hurdles must be addressed in order to enable scalable, reliable quantum-secure architectures.



Device and Modality Control. Managing a mix of classical and quantum hardware, such as routers, repeaters, detectors, and sources across multiple vendors and locations requires a hardware abstraction layer. This enables centralized, dynamic control across diverse modalities.

Low-Latency Entanglement over Multihop Networks. Long-distance quantum links often span multiple hops, introducing delays. Real-time operating systems and heralded entanglement protocols are here today that minimize latency across East-West topologies.

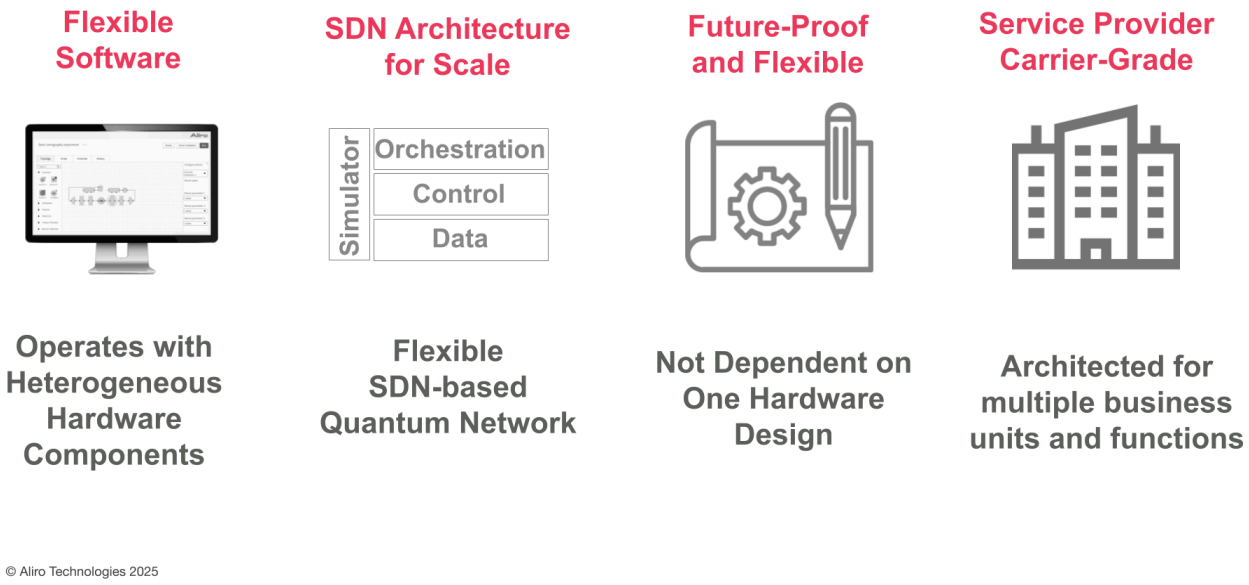
Fidelity Management. Entanglement quality can degrade due to errors in transmission. Quantum networks must incorporate protocol scheduling for multi-tenant networks, fidelity estimation, resource optimization, and error correction algorithms to ensure usable, high fidelity entanglement.

Dynamic Quantum-Safe Crypto Systems. The modern enterprise must operate in a hybrid mode. PQC should be deployed universally, with QKD and QSC layered in at the most high volume / highly sensitive data links. Dynamic cryptographic systems ensure

smooth interoperability between PQC, QKD, QSC, teleportation, OTP (one-time pad), and QRNG (quantum random number generation).

What to Look for in a Quantum Secure Data Center-to-Data Center Solution

As organizations shift toward Quantum Secure Communications, one of the most critical use cases is securing communication between data centers. Whether connecting primary and backup sites, or linking core infrastructure to regional campuses or cloud hubs, the data center-to-data center (DC-to-DC) link carries some of the most sensitive, high-volume traffic in the enterprise. However, not all quantum networking solutions are created equal.



Here's what to prioritize when evaluating your DC-to-DC options:

Flexible, Vendor-Agnostic Software. The first requirement is flexibility. Your solution should not be locked into a single hardware vendor or a proprietary stack. Look for software that supports heterogeneous infrastructure that is capable of interfacing with multiple vendors' routers, switches, and quantum devices. This is particularly important for organizations that use one vendor for campus networks and another for data centers. Your orchestration layer should unify these environments, creating consistent and symmetrical control.

Software Defined Network Architecture for Scale. The separation of data plane, control plane, and orchestration plane through a Software Defined Network (SDN)

architecture has become the de facto standard for quantum networks, mirroring best practices that have been defined over decades in the classical network space. These are now applied to quantum networking.

Future-proof: not dependent on one hardware design or hardware vendor. Changing from one topology to another topology should be straightforward. Choose a solution that remains ready to grow and evolve as your needs change, with support for the inevitable changes the network will undergo.

Service Provider Carrier-Grade. Large enterprises and public sector organizations often operate like service providers, managing multiple business units, departments, or even subsidiaries. Your quantum networking platform should be capable of managing multi-tenant environments, allocating resources dynamically, and maintaining high uptime and visibility. Look for a solution architected to support multiple business functions within one platform.

First and Next Steps

Aliro recommends a three-step journey for organizations beginning their transition to quantum networking.

1. Education. You're already educating yourself by reading this report! There is a lot of information and a wide range of resources available to you. Aliro's website has free, accessible resources such as webinars, white papers, and blog posts.
2. Design and Simulation. Using available software platforms, design and simulate a quantum network tailored to your data center architecture. This step is cost-effective, doesn't require any hardware purchase and can help identify the best components for securing your data ingress and egress.
3. Pilot and Trial. Pilot the technology in a lab environment or between two physical sites — such as between buildings or campus segments. This allows your organization to validate performance and understand the orchestration layer before implementing a broader rollout.

These first steps are accessible, low-risk, and high-impact. By starting today, you lay the groundwork for a provably secure network that scales with your mission and adapts to emerging threats.

Your Quantum-powered Secure Network

Quantum networks are more than a security upgrade; they're a strategic evolution of your IT infrastructure. The right DC-to-DC solution will not only protect your most critical data but also give you the agility to operate across diverse environments, scale as needed, and stay ahead of security threats.

Entanglement-based quantum networks are being built today by a variety of organizations for a variety of use cases – benefiting organizations internally, as well as providing great value to an organization's customers. Telecommunications companies, national research labs, and systems integrators are just a few examples of the organizations Aliro is helping to leverage the capabilities of quantum secure communications.

AliroNet® , the world's first full-stack entanglement-based network solution, consists of the software and services necessary to ensure customers will fully meet their secure networking goals. Each component within AliroNet® is built from the ground up to be compatible and optimal with entanglement-based networks of any scale and architecture. AliroNet® is used to simulate, design, run, and manage quantum networks as well as test, verify, and optimize quantum hardware for network performance. AliroNet® leverages the expertise of Aliro personnel in order to ensure that customers get the most value out of the software and their investment.

Depending on where customers are in their quantum networking journeys, AliroNet® is available in three modes that create a clear path toward building full-scale entanglement-based secure networks: (1) Emulation Mode, for emulating, designing, and validating entanglement-based quantum networks, (2) Pilot Mode for implementing a small-scale entanglement-based quantum network testbed, and (3) Deployment Mode for scaling entanglement-based quantum networks and integrating end-to-end applications. AliroNet® has been developed by a team of world-class experts.

To get started on your Quantum Networking journey, reach out to the Aliro team for additional information on how AliroNet® can enable secure communications.