Aliro™

Aliro Simulator for Quantum-secure Data Centers, HQs, & Clouds

Aliro

www.alirotech.com

Aliro Simulator for Quantum-secure Data Centers, HQs, and Clouds

Executive Summary

Advanced AI and quantum computing pose increasing threats to conventional encryption systems. The need for security solutions that counter these threats is urgent, particularly for enterprises and institutions managing network infrastructure for data centers and cloud platforms. Quantum networking, built on the principles of physics instead of relying on the hardness of math problems, has emerged as the gold standard for safeguarding high-value data traffic.

While quantum networks offer physics-backed provable security, acquiring the components to build them can be costly in both time and financial commitment. However, using a quantum network simulator can significantly reduce these costs, while simultaneously providing other benefits. Quantum network simulation is a valuable tool for designing, validating, and deploying these next-generation secure networks.

Investing in quantum network simulation today lays the foundation for secure operations that can expand as confidence and capabilities grow. With its ability to reduce R&D costs, enhance design integrity, and accelerate deployment timelines, Aliro Simulator empowers organizations to transition from exploration to implementation with less risk.

Aliro Simulator offers a flexible digital environment for simulating network behavior at different scales, modeling noise and environmental factors, and testing protocols. By simulating how quantum systems behave in real-world conditions, Aliro Simulator validates performance of the network and helps engineers and technologists understand the trade-offs of different configurations.

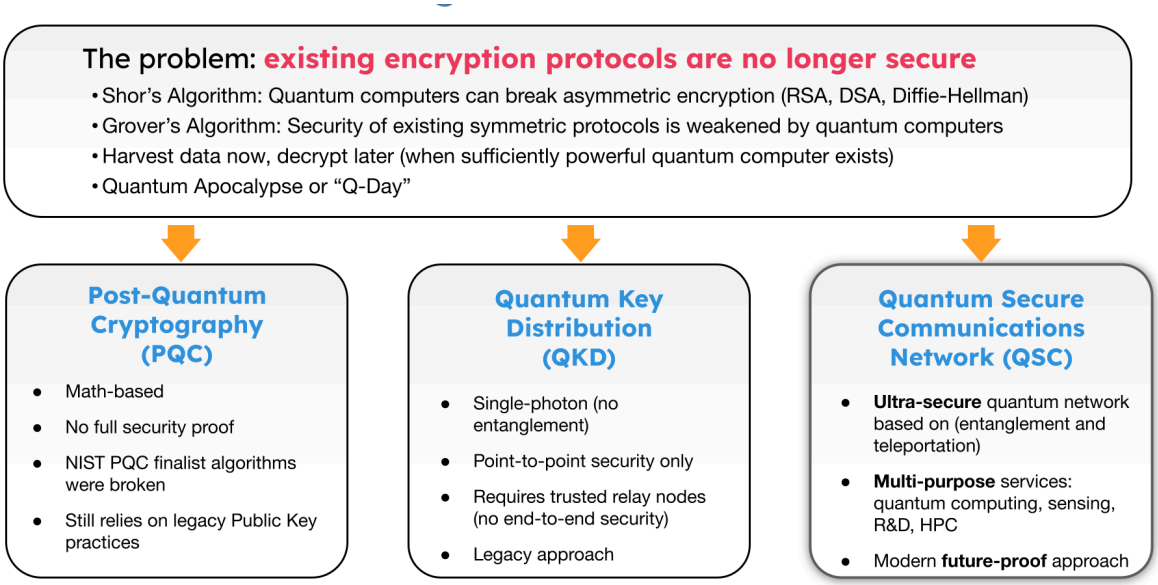
Organizations that lay the foundations of their quantum network today will be better positioned to adapt as quantum technologies become mainstream. Aliro enables organizations to leverage early preparations with tools designed for long-term adaptability.

The Quantum Threat and the Quantum Solution

As quantum computing advances, classical encryption protocols (especially those underpinning public key infrastructure) are increasingly vulnerable. Even before a cryptographically relevant quantum computer arrives, Harvest Now Decrypt Later (HNDL) attacks are already a serious threat. In HNDL attacks, adversaries intercept and store encrypted data now with the intention of decrypting it once quantum computers are capable.

This reality presents a high-stakes challenge for organizations that manage or rely on data center interconnects. Data center networks often carry highly sensitive information that must remain secure for long periods of time, making mitigating the risk to these links a high priority. There are

several protections available today that can protect sensitive data from HNDL attacks and the arrival of powerful quantum computers: Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Secure Communication (QSC).



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 in public key 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 finalized a set of candidate standards following rigorous public testing. Several early contenders failed, with some unable to withstand basic decryption attacks using conventional laptops. PQC will become a pervasive tactic for protecting data, deployed across the entire network; this is the baseline of quantum secure infrastructure. PQC is an essential first step for data center links, but as a mathematical approach, it may be vulnerable to future attacks we aren't aware of today.

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 what is referred to as prepare-and-measure QKD: a point-to-point security mechanism that requires trusted relay points to extend the distance of the links. Some vulnerabilities are introduced by these trusted relay points due to data being exposed in the clear at each relay. While valuable for some links, QKD's end-to-end security limits make it less ideal for high-capacity, multi-node data center links. For those links where QSC is not feasible but physics-based protections are desired, QKD can be a helpful method.

Quantum Secure Communications (QSC). QSC is an ultra-secure physics-based methodology that leverages entanglement and teleportation. This is the most secure implementation for

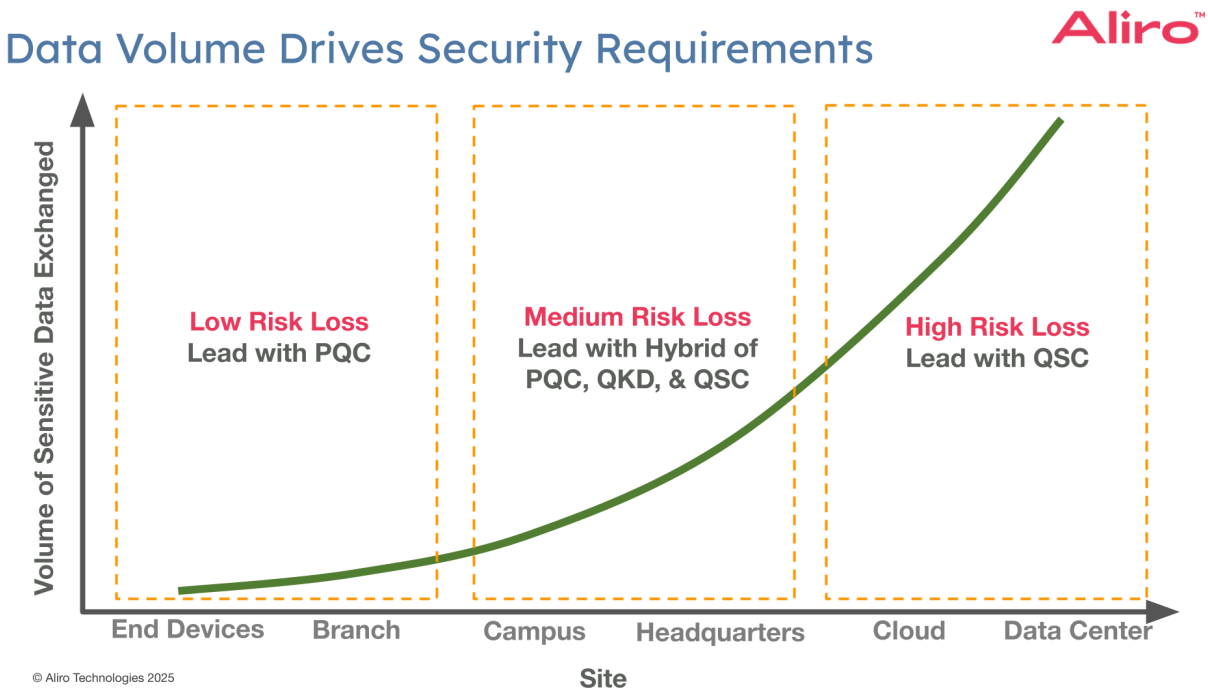
protecting the high-volume links that carry the most sensitive data. QSC is modern and future-proof, and because it's entanglement-based this technology can carry out other applications such as interconnecting quantum computers, connecting distributed quantum sensors with one another, and other applications that we're not even aware of today. QSC is well suited for data center interconnects with the most demanding confidentiality requirements, and also supports future applications such as interconnecting quantum processors or distributed quantum sensors that might add to future data center capabilities.

The timeline to Q-Day, the day a cryptographically relevant quantum computer (CRQC) comes online, continues to accelerate. Since the advent of Shor's algorithm in 1994, researchers and governments have acknowledged the need to replace vulnerable encryption systems. NIST began the formal process of standardizing post-quantum cryptography (PQC) in 2016. In 2019, Google achieved quantum supremacy. And more recently, research from China and new hybrid quantum-classical algorithms suggest that the number of qubits needed to break RSA-2048 could be significantly lower than previously estimated. While conservative estimates project a CRQC to be 10 years away, aggressive forecasts suggest it could arrive in as little as 3–5 years. Gartner recently estimated that a CRQC could arrive by 2029, and that asymmetric cryptography could be fully broken by 2034. For organizations that operate mission-critical data center infrastructure, waiting for this inevitability is a risk not worth taking. But what can be done now to prepare?

Critical communication paths such as data center-to-data center (DC-to-DC), data center-to-headquarters (DC-to-HQ), and headquarters-to-cloud (HQ-to-Cloud) could be protected at the highest level of security using QSC. These links often carry highly sensitive data and require long-term confidentiality that QSC provides. Organizations responsible for securing data center infrastructure can proactively prepare for imminent sophisticated threats by using a quantum network simulator to create and test a Quantum Secure Communications network plan. Simulators like the Aliro Simulator can model entanglement-based networks, evaluate performance under varying conditions, and optimize integration with existing infrastructure. By enabling experimentation without physical risk, Aliro Simulator provides helpful analysis on how to protect data beyond Q-Day. As the countdown to Q-Day accelerates, quantum network simulation lays the foundation for quantum-powered security.

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.

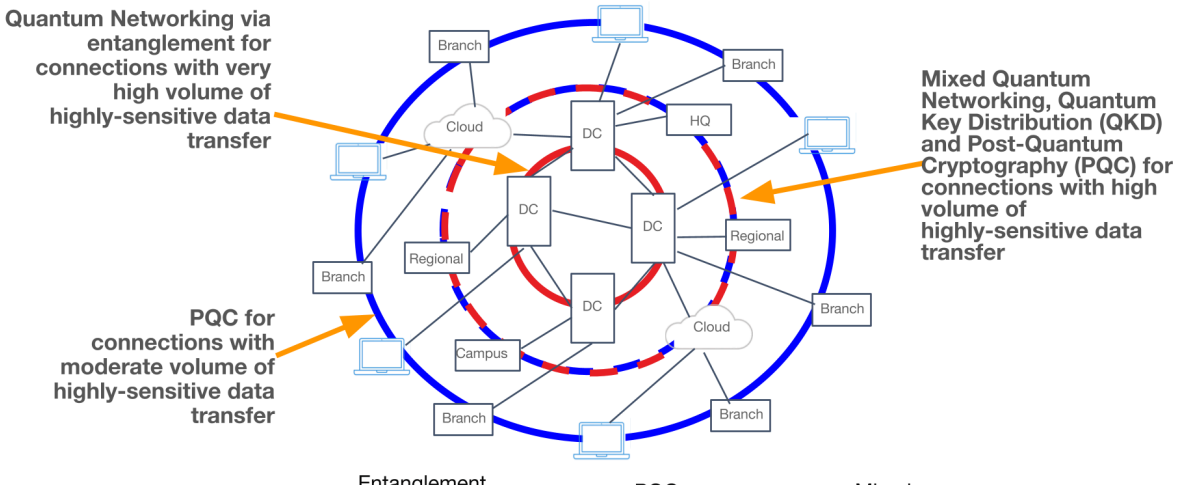
Branch offices and remote sites represent a step up in the scale and criticality of data, and a step up in risk. These locations may host dozens to hundreds of employees, each engaging in daily operations that generate sensitive client, logistics, or financial data. The volume of information justifies 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.

Looked at as a series of concentric circles, a defense-in-depth model that addresses modern network complexity is focused on 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.

A Phased Approach to Quantum-powered Security

For data center operators, integrating quantum networks into existing links can appear daunting due to complexity, cost, and challenges in implementation. Designing quantum networks requires precision in modeling component behavior, noise and environmental factors, protocol and device compatibility, and performance scalability. A phased, strategic approach makes adoption of quantum-powered security both practical and scalable. The first step in a phased approach is simulation.

Quantum network simulators such as Aliro Simulator play a critical role in the planning phase. By modeling entanglement-based network topologies, testing protocol configurations, and assessing performance under realistic network conditions, a simulator helps organizations design, validate, and optimize quantum network behavior for their unique situation. Incremental expansion of the quantum network can then add more interconnects, cloud gateways, or geographically distributed facilities. This simulation-led approach reduces risk, aligns with capital planning cycles, and helps organizations build internal quantum expertise over time.

Role of the Quantum Network Simulator

Quantum network simulation is the foundation for planning and validating the integration of quantum networking with data center-to-data center (DC-to-DC), data center-to-headquarters (DC-to-HQ), and headquarters-to-cloud (HQ-to-Cloud) architectures. Simulation enables:

- Topology planning. Modeling the existing fiber infrastructure and characteristics your quantum network will run on.
- Hardware modeling. Evaluating entangled photon source placement, quantum memories, and photonic interfaces it different levels of abstraction: from individual device behavior up to a wide area network.
- Performance optimization. Assessing latency, fidelity, key generation rates, and fault tolerance.
- Integration strategies. Testing how quantum systems interoperate with existing classical encryptors, routers, and DWDM systems as well as interoperability between quantum network devices.

Aliro Simulator supports modeling from the smallest photonic component to full-scale multi-site quantum-secure networks.

Aliro Simulator: Advancing Quantum Networking Through Comprehensive Simulation

Entanglement-based quantum networking holds immense potential for secure communication, enhanced cloud access, and networked quantum computers. However, developing and deploying quantum networks presents significant challenges, demanding meticulous design, validation, and implementation. Aliro addresses these challenges with its robust Aliro Simulator, a scalable cloud platform and simulation pipeline designed to facilitate the development and optimization of quantum networks. This white paper provides an overview of the Aliro Simulator, highlighting its features, capabilities, and benefits for researchers and developers in the quantum networking space.

Key Features and Capabilities

Aliro Simulator offers a comprehensive suite of tools and functionalities to support the simulation and analysis of quantum networks. Key features include:

- Discrete Event Simulation: The simulator supports discrete event simulation, allowing users to model the dynamic behavior of quantum network components and protocols over time.
- Quantum Simulation: At its core, the Aliro Simulator provides quantum simulation capabilities, enabling the modeling of quantum phenomena and interactions within the network.
- Quantum Networking Protocols: The simulator supports the implementation and testing of various quantum networking protocols, allowing for the evaluation of their performance and effectiveness.
- Quantum Network Components and Noise Modeling Library: A comprehensive library of quantum network components and noise models is available, enabling users to create realistic simulation environments and analyze the impact of noise on network performance.
- Python Simulation Framework: The simulator leverages a powerful Python simulation framework, providing a comprehensive API for simulating network devices and protocols. The framework also includes tools for data collection, processing, and visualization.
- Scalable and Swappable Backend: The simulator offers a scalable and swappable backend, allowing integration with various quantum simulators, such as Cirq, QuTIP, and QSim. It supports multiple state representations, including State Vector, Density Matrix, and Stabilizer, and can scale on the cloud using parallel processing or GPU acceleration.
- Scalable Cloud Platform and Simulation Pipeline: The simulator is built on a scalable cloud platform, enabling efficient execution of complex simulations. Its streamlined pipeline simplifies the setup, execution, and visualization of simulation results.

Simulation-Aided Design

The Aliro Simulator plays a critical role in simulation-aided design, particularly for Entanglement Purification and Photon Sources (EPPS). By providing a virtual environment for testing and refining EPPS designs, the simulator enables developers to optimize performance and identify potential issues before physical implementation.

Design Validation and Optimization

Theoretical formulas for quantum network behavior can quickly become intractable, making simulation essential for design validation.
The Aliro Simulator facilitates:

- Verification: Ensuring that the network design aligns with theoretical principles and specifications.
- Sanity Checks: Identifying potential flaws or inconsistencies in the design.
- Optimization: Fine-tuning parameters and configurations to maximize network performance.
- Parameter Setting: Determining optimal values for network parameters.

- Design Choices: Evaluating different design options and their impact on network behavior.
- Alignment with Experimental Data: Comparing simulation results with experimental data to validate the accuracy of the model.

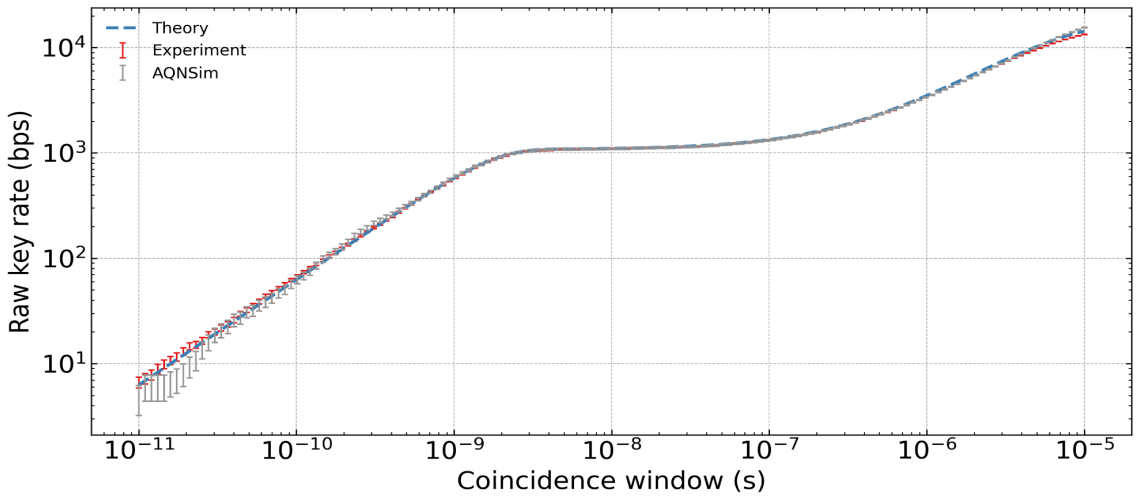


Figure 1. Comparison of Theoretical, Experimental and Aliro Simulation Results for Key Rate

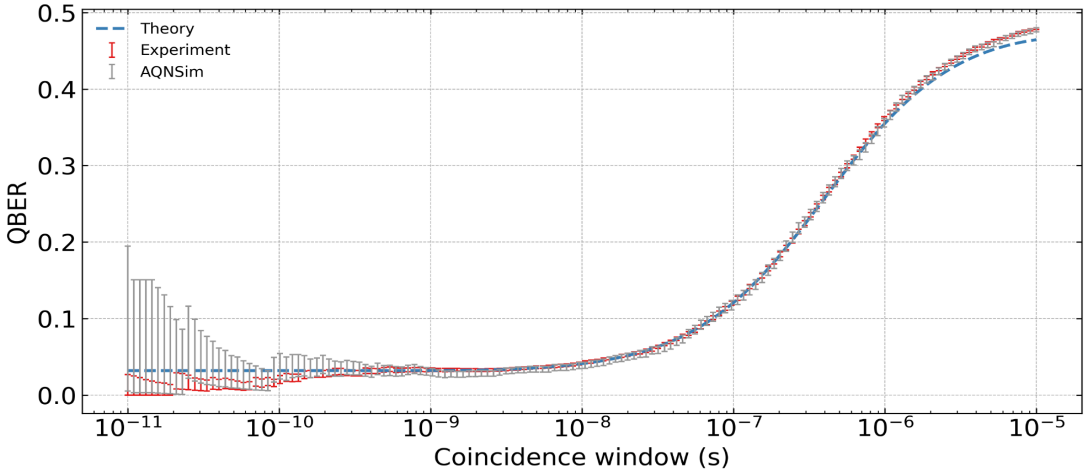


Figure 2. Comparison of Theoretical, Experimental and Aliro Simulation Results for Qubit Error Rate

Benefits of Using Aliro Simulator

- Accelerated Development: The simulator significantly reduces the time and cost associated with quantum network development by enabling virtual testing and optimization.
- Improved Design Quality: Simulation helps identify and address potential issues early in the design process, leading to higher-quality and more robust network designs.

- Enhanced Understanding: The simulator provides valuable insights into the behavior of quantum networks, enhancing understanding and facilitating innovation.
- Risk Mitigation: By enabling thorough testing and validation, the simulator helps mitigate risks associated with deploying complex quantum networks.
- Interoperability: The simulator's scalable and swappable backend ensures interoperability with various quantum simulators and state representations.

Conclusion

Aliro Simulator is a powerful tool for advancing quantum networking research and development. Its comprehensive features, scalable platform, and robust simulation capabilities empower researchers and developers to design, validate, and optimize quantum networks effectively. Aliro simulation results provide a tight correlation with both theoretical and hardware-based experimental results. By leveraging the Aliro Simulator, organizations can accelerate their journey towards realizing the full potential of quantum networking and its transformative applications.

A Full-stack Solution for Quantum Networking

Entanglement-based secure 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, intelligence organizations, and systems integrators are just a few examples of the organizations Aliro is helping to leverage quantum networking.
Building entanglement-based quantum networks is no easy task. It requires:

- Emerging hardware components necessary to build the quantum network.
- The software necessary to design, simulate, run, and manage the quantum network.
- A team with expertise in quantum physics and classical networking.
- Years of hard work and development.

This may seem overwhelming, but Aliro is uniquely positioned to help you build your quantum network. The steps you can take to ensure your organization is meeting the challenges and leveraging the benefits of the quantum revolution are part of a clear, unified solution already at work in quantum networks like the EPB Quantum Network℠ in Chattanooga, Tennessee.

AliroNet™, the world's first full-stack entanglement-based quantum network solution, consists of the software and services necessary to ensure customers will fully meet their quantum networking goals. Each component within AliroNet™ is built from the ground up to be compatible and optimal with quantum 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 quantum networks, (2) Pilot Mode for implementing a small-scale quantum network testbed, and (3) Deployment Mode for scaling quantum networks and integrating end-to-end applications.

AliroNet™ has been developed by a team of world-class experts in quantum physics and classical networking. To get started (or continue on your quantum journey), reach out to the Aliro Quantum team for additional information on how AliroNet™ can enable your quantum network.

info@alirotech.com www.alirotech.com