QuSecure and Graphiant: Futureproofing Networking Cybersecurity with Crypto-Agility

Executive Summary

As the digital landscape evolves, the need for robust cybersecurity measures becomes increasingly critical. Nearly everyone in the world has or will be affected by breaches of digital information. Even with today's cyber defenses, no business or government agency can fully protect their data. At the same time, networks are more complex making them harder to manage, which requires new solutions for network optimization and security. The advent of quantum computing presents both opportunities and significant challenges. Existing network encryption methods are vulnerable to quantum attacks, necessitating the development of post-quantum cybersecurity solutions. QuSecure, a leader in post-quantum cybersecurity, offers a suite of products designed to protect against these emerging threats empowering organizations to remain agile in an evolving technology and threat landscape. By integrating QuSecure's products with the Graphiant platform, organizations can achieve a secure, scalable, and efficient network infrastructure capable of withstanding quantum-era risks.

Purpose of This White Paper

In this paper, we describe how Graphiant's Network Edge combined with QuSecure's postquantum cryptographically agile solutions provides a fast, easy and cost-effective way to build and secure enterprise networks. Integrating QuSecure's post-quantum products with Graphiant's platform provides comprehensive protection against a wide range of cyber threats. QuSecure's crypto-agile PQC solutions offer a robust defense against quantum attacks, while Graphiant's network security features protect against classical threats. The combined solution ensures the most advanced end-to-end encryption for data in transit.

The Graphiant Platform - Network Innovation and Advanced Routing

Modern infrastructure is paramount in a time when applications are rapidly built and deployed. Large datasets are transported between data centers and clouds, and the rapid acceleration in artificial intelligence capabilities is accelerating business.

Our classical data networks were built statically for a time when applications and their data sets were limited and resided in a fixed location. We built networks to ensure the business application can be consumed by a human operator performing a series of limited digital interactions.

This doesn't work anymore. The world is more dynamic than ever. Our digital resources have multiple forms and must service capabilities within our and our partners' networks, from cloud to data center to edge. Our digitally transformed world requires us to provision these connections

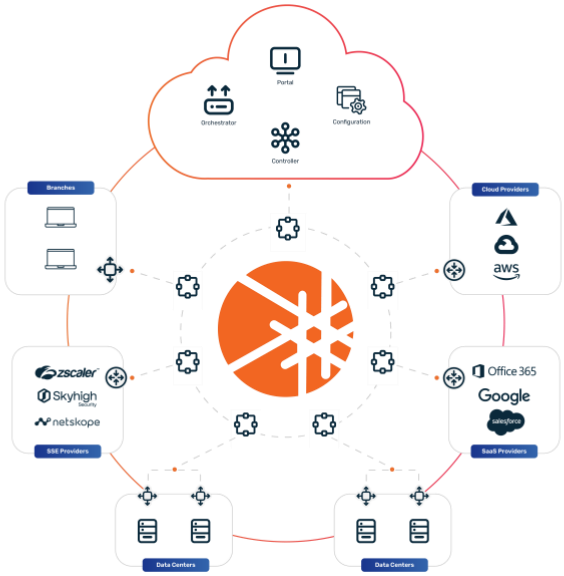
faster, with mechanisms to guarantee the instantiation of data transport with defined characteristics of quality and security.

Graphiant is the new modern software stack that completely changes how AI networks are built, replacing classical networks with a scalable, secure, and highly cost-effective cloud-delivered Network-as-a-Service (NaaS).

Graphiant:

- Provides a **single connectivity solution** for all resources, including clouds, private applications, business partners, and data centers.
- **Eliminates the complexity** of older technologies.
- **Delivers the highest privacy and compliance** with end-to-end encryption.
- **Guarantees delivery** with end-to-end SLAs for applications.

Graphiant's unique architecture keeps control in the cloud rather than individual devices. This allows Graphiant’s global distributed private core to be highly scalable and cost-effective, enabling customers to simply connect and consume network services.



The main components of the Graphiant NaaS are as follows:

- The Graphiant Core: a natively multi-tenant core that handles reachability to Graphiant services. It is a high throughput, guaranteed delivery, stateless environment that delivers ubiquitous, any-to-any connectivity.
- The Graphiant Edge: a software package deployed in virtual or bare metal formats on compute at sites to deliver Graphiant's connectivity services to users and applications.

- The Graphiant Portal: a simple operational dashboard with complete API control from where the network can be entirely programmatically operated to initiate connectivity, order new sites, set policies, and buy services.

The Stateless Core is central to Graphiant's architecture. It provides private links to enterprise resources, cloud services, and SaaS providers and delivers SLA and traffic visibility for traffic on the core. All data, including customer IP information, is encrypted using NIST-certified algorithms to meet the highest encryption standards. The core provides resilience and trust since it does not carry any customer information, especially customer data encryption keys.

Quantum Computing and the Threat to Modern Encryption

Introduction - The Quantum Computing Revolution

Quantum computing represents a paradigm shift in computational power. Leveraging the principles of quantum mechanics, quantum computers use qubits to perform calculations at speeds unattainable by classical computers. This breakthrough has significant implications for various fields, including cryptography, where it poses both opportunities and threats.

The Need for Enhanced Cybersecurity

The principles that make quantum computing powerful also render traditional encryption methods obsolete. As organizations digitize their operations, the need for advanced cybersecurity measures becomes imperative. QuSecure's post-quantum cryptographic solutions offer a robust defense against these threats. Quantum computers are powerful machines that operate differently than the standard computers of today. Most of us are familiar with the idea that our current computers and devices use integrated circuit (IC) chips using 0's and 1's. For the most part this construct has served us well whether we are using desktops, laptops, phones or large servers. However standard computers struggle with certain sets of problems, one of which happens to be the base of the current cryptography that protects our data today. As an example, this article you are reading was provided to you via the Internet from a set of servers and is protected by public key encryption. The data that makes up this article and the Internet it traveled across uses encryption protected by a mathematical equation using large numbers and the factors that go into those numbers. Also called Prime Factorization, this math problem is unbelievably difficult for classical computers to solve. In other words, even extremely powerful classical computing machines like super computers cannot crack this prime factor-based encryption.

However, quantum computers operate differently. Using a subatomic property called superposition, quantum computers can process problems like prime factorization and multivariate problems due to how they process data and the way they can be programmed. Unlike our classical computers where the base elements must be zero or one, superposition allows quantum computers to take advantage of a base element being zero, one and anything in between, all at the same time.

While quantum programming enables great opportunities for humanity, it is understood that adversarial nation-states are building quantum computers to use as weapons. Quantum computing investments are very large and with this amazing power, quantum computers can handle problem sets not solvable by classical computers, including decrypting communications and data. The first nefarious nation-state that brings a quantum computer online with enough power to crack encryption ***will have global domination at its fingertips***. All the private and secret information traveling over the Internet will be available to anyone who has this compute power. This includes national secrets, healthcare data, financial and banking information, as well as access to infrastructure like energy grids, satellite communications and water supplies. Worse yet, it is heavily documented that some nations are stealing vast amounts of data which is currently encrypted but will be decrypted when a quantum computer with enough power is available. Sometimes called "Steal Now, Decrypt Later" (SNDL) this describes stealing and storing data for a future date when there are systems that can decrypt, view and operationalize that data. Much of the data created today needs to have decades of secrecy and therein lies the problem. Most data sets mentioned above would need to remain secret for 25-75 years and would be valuable if cracked sooner. But if stolen now and decrypted within a few years by a quantum computer, an adversary would have the capability to operationalize that data to disrupt society, steal intellectual property, gain financially or increase the chances of winning a war. ***In other words, quantum computers have the potential to rebalance global power.***

Arthur Herman of the Hudson Institute directed a group to study the effects of quantum computing attacks on various key systems. His methodology used an econometric model with over 10,000 data points to provide the best assessment of the effects of quantum computing if used as a weapon. In these studies, the Hudson Institute found that quantum computing attacks on our banking and finance systems, cryptocurrencies and more would cause trillions in damage with a single attack. “Our preliminary econometric research at the Hudson Institute’s Quantum Alliance Initiative indicates that the cost of a quantum computer attack on our financial system would be catastrophic—far more than a successful conventional cyberattack,” said Herman in his May 2021 Forbes article entitled, “Getting the Big Banks to Confront the Quantum Challenge.” He goes on to say that a single quantum computing breach “would cause a cascading financial failure costing anywhere from $730 Billion to $1.95 Trillion.” Any successful attack of this magnitude would change the way of life as we know it in the United States, not only from the sheer loss and recovery necessary to stabilize, but also in the dramatic and fundamental loss of trust.

The Quantum Threat Landscape - Vulnerabilities of Traditional Cryptography

Traditional cryptographic methods, such as RSA, ECC, and DSA, rely on the computational difficulty of certain mathematical problems (e.g., integer factorization, discrete logarithms) to ensure security. While these methods are secure against classical computers, quantum computers can exploit their vulnerabilities. Quantum algorithms like Shor's algorithm can efficiently solve problems that underpin classical cryptographic systems. For instance, Shor's algorithm can factorize large integers exponentially faster than the best-known classical algorithms, rendering RSA encryption insecure. Organizations across the public and private sectors depend on the ability to securely communicate data over computer networks. By using Shor's algorithm, a quantum computer of sufficient size can efficiently break public-key algorithms such as RSA, ECDH, and ECDSA which secure these network communications today. As a result, organizations will need to replace all instances of vulnerable cryptography to protect their own and their customers' data-in-transit.

Emerging Threats - Data Harvesting for Future Decryption

SNDL makes the immediate adoption of post-quantum cryptographic solutions critical to safeguarding long-term data security. Post-quantum cryptographic algorithms, such as latticebased, hash-based, code-based, and multivariate-quadratic-equations-based cryptography, are designed to be secure against both classical and quantum attacks. These algorithms are the cornerstone of QuSecure's product offerings.

QuSecure's Post-Quantum Cybersecurity Products

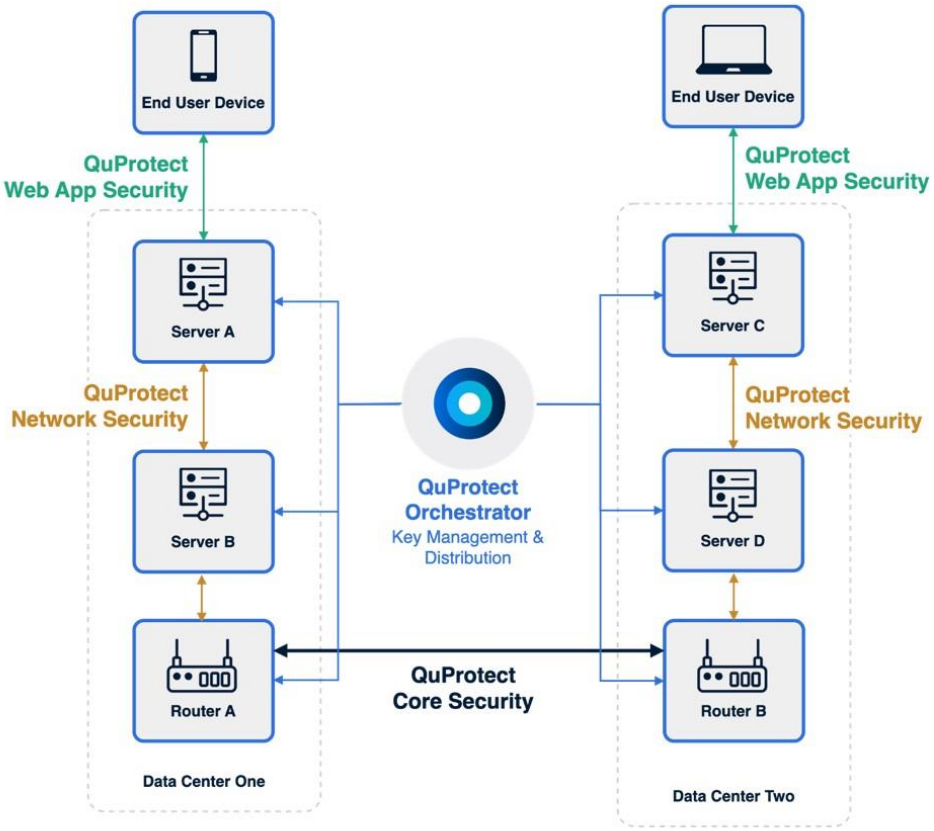
QuSecure's QuProtect platform is a comprehensive suite of post-quantum cryptographic solutions designed to safeguard data across various platforms and applications. It includes quantumresistant algorithms, cryptographic agility, key management systems, and secure communication protocols. QuSecure enables visibility into cryptography in use – a new level of insight. QuSecure features include:

Centralized Control and Management - QuSecure provides centralized control of quantum resilient cryptography, which is ideal for managing and updating cryptographic protocols across the network. Post-quantum algorithms can be implemented and updated centrally, ensuring uniform security policies.

Cryptographic Agility - Cryptographic agility refers to the ability to swap vulnerable or otherwise non-optimal cryptography with minimal disruption to operations. QuSecure enables Graphiant/QuSecure organizations benefit from 3 forms of agility:

- Algorithm agility – hot-swap cryptographic algorithms with a mouse-click
- Protocol agility - means the ability to upgrade from a vulnerable protocol version, such as migrating from TLS 1.0 to TLS 1.3.
- Implementation agility - means quickly patching vulnerable algorithm implementations

Decoupling Cryptographic Functions from Applications - Using QuSecure, PQC algorithms can be integrated into Graphiant's solution by decoupling cryptographic functions from applications. This allows for flexible and dynamic management of cryptographic methods through centralized control mechanisms.



Automation and Orchestration - Automation is a critical aspect of both SDNs and post-quantum cryptography. By integrating QuSecure. post-quantum algorithms will be centrally deployed allowing for the maintenance of cryptographic keys.

QuSecure Provides PQC Visibility and Monitoring - QuSecure provides enhanced visibility into network traffic and security postures to monitor the effectiveness and integrity of post-quantum cryptographic implementations.

Dynamic Policy Enforcement - QuSecure can dynamically enforce security policies for implementing post-quantum cryptographic measures. This allows for responsive adjustments to security protocols based on real-time threat intelligence.

Integration with Existing Infrastructure - QuSecure integrates with existing infrastructure and cybersecurity systems by leaving existing encryption in place. Using QuSecure, post-quantum cryptographic algorithms can be deployed alongside current cryptographic systems, ensuring backward compatibility and a smooth and fast transition.

Graphiant and QuSecure

Graphiant's network services use the NIST-approved RSA algorithm for public key encryption to ensure trusted authentication and to deliver end-to-end encryption for critical data. This encryption suite is one of the most widely deployed and trusted mechanisms for guaranteeing privacy. This singularly important capability created the means for our modern global digital economy. This algorithm, though, is reaching the end of its lifecycle as the advent of quantum computing opens the possibility that this algorithm will be broken within the next decade. In anticipation of such an event, malicious entities have been conducting long-term efforts to harvest data now in the hopes of being able to decrypt sensitive data once the process of breaking RSA becomes computationally more viable.

For Graphiant, this means ensuring that the data transports are being built for the future by incorporating Post Quantum Cryptography and emerging FIPS compliance in mind. Furthermore, QuSecure's crypto agility ensures that the newly certified algorithms can be rapidly deployed while keeping the network and encryption decoupled to allow for independent changes in each.

Graphiant's software architecture introduces new techniques that remove peer-to-peer control plane relationships while establishing a peer-to-peer encrypted data plane. Utilizing a central control framework with a pairwise data plane between endpoints for symmetric pairwise encryption reduces the potential attack surface for harvesting the initial authentication exchanges that could be broken. The centralized control framework also gives administrators the flexibility to deploy new cryptographic algorithms for establishing trusted authentication without the possibility of degraded cipher attacks.

Graphiant utilizes this control delivery capability to integrate with third-party solutions, enabling organizations to enhance network encryption capabilities. Graphiant's separation of elements creates a simple integration pathway to deliver post-quantum cryptographic capabilities into the data network infrastructure. Graphiant provides a mechanism by which the Graphiant Portal can establish a tenancy relationship with a PQC key provider like QuSecure, that can program the necessary keystores on the Graphiant Edge to utilize PQC-derived keys instead of classical RSA keys and protect against any brute force or harvest now, decrypt later attacks.

This allows Graphiant to maintain its strong posture of never having access to keys, generated or otherwise, that are programmed into the cryptographic keystores at the Edge. Graphiant utilizes the new algorithms to establish new trusted connections with the Graphiant Stateless Core to create a global wide area network that has predictable, defined paths to protect against man-inthe-middle and denial of service attacks. This ensures that even with those kinds of attacks, and with intermediate data harvesting attacks, the data itself remains secured with end-to-end encryption using post-quantum keys from QuSecure for a network that is ready to meet the newly defined standards for highly regulated, sensitive data environments now and introduce crypto-agile foundations for the future.

About QuSecure

QuSecure(https://qusecure.com) is a global leader in post-quantum cybersecurity, dedicated to developing innovative solutions that protect against quantum and classical threats. With extensive commercial and federal-level installations, QuSecure is at the forefront of the postquantum security revolution.

Key Achievements

Industry Recognition: QuSecure has received numerous accolades from institutions such as Frost & Sullivan for its contributions to post-quantum cybersecurity.

Commercial and Federal Installations: Extensive deployment across commercial enterprises and federal agencies in addition to several SBIR awards, including an SBIR Phase III.

Collaborations: Partnerships with leading companies like Accenture and Cisco to produce cutting-edge cybersecurity products and enterprise solutions.

About Graphiant

Graphiant (https://graphiant.com/) is a pioneering networking company that delivers advanced network solutions to optimize performance, scalability, and security. Its platform enables seamless integration with third-party solutions, providing a flexible and robust infrastructure for modern organizations.

Key Achievements

Innovative Networking Solutions: Recognized for its innovative approach to networking, enhancing performance and security.

Scalability and Flexibility: Designed to accommodate the growing needs of modern enterprises.

Industry Collaborations: Collaborations with leading cybersecurity and technology companies to deliver comprehensive solutions.