Preparing for Quantum Attacks: Securing Critical Communications

SENTRIQS

EXECUTIVE SUMMARY

Driven by the expanded role of mobile devices in business workflows, and heightened by the COVID-19 pandemic that fueled wide scale acceptance of hybrid/remote workspaces, instant messaging (IM) emerged as an essential communication tool in the workplace.

Within critical sectors such as energy, healthcare, finance, and emergency services, these messaging platforms are now vital for rapid decision-making and improved operational efficiency.

However, instant messaging platforms pose significant cyber security threats to critical sector organizations. Increasingly, cyberattacks targeted at these sectors have the potential for large-scale damage. Quantum computing heightens these threats, making the risk and the urgency far more immediate.

Quantum computing is a paradox in the security paradigm. While quantum has the potential to improve cybersecurity, it also threatens its foundations. Experts predict that Q-Day, when quantum computers will be able to break traditional security encryption processes, may occur within a decade.

Due to the evolving nature of cyber security attacks, organizations will benefit from continued security advancements to meet ongoing threats. Messaging Layer Security (MLS) is one example of these advancements, offering scalable and ultra-secure protections for communication.

Government officials have advised organizations to adopt quantum-safe security measures using Post-Quantum Cryptography (PQC) protocols to prepare for quantum threats. Considering this, in August 2024, NIST announced three post-quantum cryptography standards based on the ML-KEM, ML-DSA, and SLH-DSA algorithms, respectively to protect digital communications against quantum attacks.

Software pioneer SENTRIQS developed the GLYPH messaging protocol to deliver quantum-safe protections for business collaboration. Combining MLS and PQC through a highly-agile and crypto-efficient architecture, the GLYPH Protocol accelerates organizational productivity while delivering superior communications safeguards against quantum threats.

TABLE OF CONTENTS

INTRODUCTION

> The modern work environment has moved beyond traditional office spaces with legacy wired communications. Today's workforce is comprised of digital natives who use mobility for rapid information management across multiple networks.
>
> – **Future of Secure Work, ATARC White Paper, March 2024**

The Rise of Instant Messaging

Over the past decade, organizations have moved beyond email and teleconferencing for business communications, relying on instant messaging and video "huddles" for immediate engagement and improved collaboration.

This shift toward broad adoption of IM and video collaboration was fueled by two major trends: 1) the expanding role of mobile devices in business workflows, and 2) the ballooning role of remote working in the new office paradigm. Mobile devices have become vital to modern business workflows, enabling greater flexibility, efficiency, and communication. As businesses increasingly adopt remote and hybrid work models, mobile devices allow employees to remain productive from virtually any location, helping them manage tasks, communicate in real-time, and access essential cloud-based tools.

This transition has been accelerated by the pandemic, which highlighted the need for seamless mobile communication and remote accessibility to maintain operations and ensure efficiency. Businesses that effectively

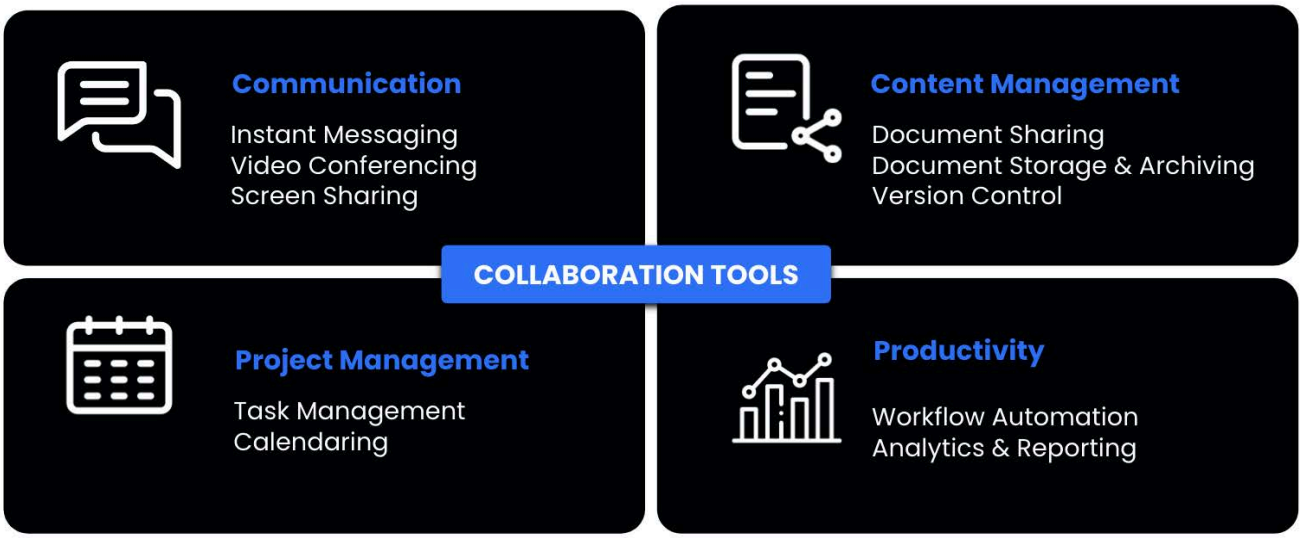
integrate mobile devices into their workflows benefit from improved decision-making, faster response times, and enhanced agility, allowing them to stay competitive in a rapidly evolving market.

The COVID-19 pandemic accelerated the adoption of messaging platforms with the sudden necessity of remote working. Post-pandemic, work has normalized, but organizations have largely held onto either a remote or hybrid work environment, with instant messaging becoming essential for conversations with colleagues, customers, investors, vendors, and partners.

In a 2023 poll[1], consulting firm Envoy found that 80% of companies surveyed were reconsidering their plans to return employees to the office full-time. Indeed, a 2023 McKinsey report[2] stated that hybrid work will continue for the foreseeable future, with a majority (56%) of office workers using hybrid work arrangements.

The popularity of messaging apps means that employees are already comfortable using them inside and outside the office. Top mobile messaging platforms like Signal, WhatsApp, WeChat, and Facebook Messenger boast billions of active users. The overwhelming familiarity with these consumer apps has blurred the lines between personal and business communications. Younger employees tend to be comfortable switching between approved and informal communication platforms. Executives, too, rely on secure messaging apps for business communications, often driven by the need to share time-sensitive information and protect important conversations.

In short, instant messaging/meetings align with the modern organizational ethos, viewing collaborative and asynchronous work as conducive to organizational health and higher productivity[3].



This growing integration of instant messaging and collaboration platforms into business workflows raises significant security concerns. These casual communication channels potentially can expose financial data, healthcare information, and corporate intellectual property to cybercriminals. Greater safeguards are required to protect all organizational assets, especially since the wide scale use of messaging platforms for business communications cannot be easily reversed simply by issuing new policies and management threats.

Benefits of instant messaging platforms

- **Real-time Communication:** Allows quick, immediate exchanges, faster response times, and more agile operations.
- **Enhanced Collaboration:** Supports the sharing of files, links, updates, and the creation of online groups and workspaces.
- **Cost Efficiency:** Replaces telephone services and in-person meetings with customer live chat messaging and videoconferencing.
- **Flexibility and Accessibility:** Connect team members from any location with an internet connection.
- **Record Keeping and Traceability:** Archives files and previous conversations.
- **Breaking Down Silos:** Strengthens employee engagement and supports organizational culture.

Instant Messaging/Meetings for Critical Sectors

When considering a nation's critical infrastructure, common perceptions may include power grids, interstate highways, or navigable waterways. However, cybersecurity professionals adopt a broader definition of critical infrastructure sectors when addressing security risks. This paper utilizes this broader perspective referring to them as "critical sector(s)." The image below identifies the sectors included in this definition.[4-10]

Critical sector industries and institutions play a crucial role in the interconnected ecosystem of national security, the economy, and public health. Threats and destabilizing events directed at these sectors, therefore, can have national significance. As a result, critical sector systems must respond immediately to emergencies and disruptions to mitigate any operational impairments.

The expansive scale of these critical sectors can complicate security measures. Headquarters' staff need to communicate with teams in the field, often in remote locations or across vast geographic areas. Organizational scale also is an issue, with efforts coordinated across multiple departments, and increasingly, multiple governmental jurisdictions, often on separate communication channels and platforms.

Rapid, secure, and effective communication for threat detection, assessment, evaluation, and dissemination among key stakeholders is vital for safeguarding critical infrastructure. Instant messaging/meeting platforms, therefore, are attractive to critical sector organizations, given the need for real-time communication and quick decision-making among widely distributed and highly disparate teams.

Problem	Instant Messaging Solution	Benefits
Slow response time in emergencies	Real-time messaging and alerts	Reduces response times to help mitigate damage
Complex coordination across diverse locations	Group chats, videoconferencing and file sharing	Seamless team coordination for improved project management
Regulatory compliance demands	Archiving for record-keeping and audits, controlled access	Helps companies adhere to safety, privacy and security standards

Cybersecurity for Critical Sectors

> "China's hackers are positioning on American [critical] infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities"
>
> – **US FBI Director Christopher Wray testifying to the US Congress.**

The clear operational risks facing the world's critical sector organizations is heightened by their growing vulnerability to cyber terrorists. Critical sector institutions are frequent targets of sophisticated cyberattacks precisely because these attacks can inflict

widespread damage. This means attackers' malicious intent can cause widespread damage and involve significant ransom demands. Complex geopolitical matters can result in state-sponsored cyberattacks on critical sectors, and involve highly organized cyber espionage and disruption campaigns.

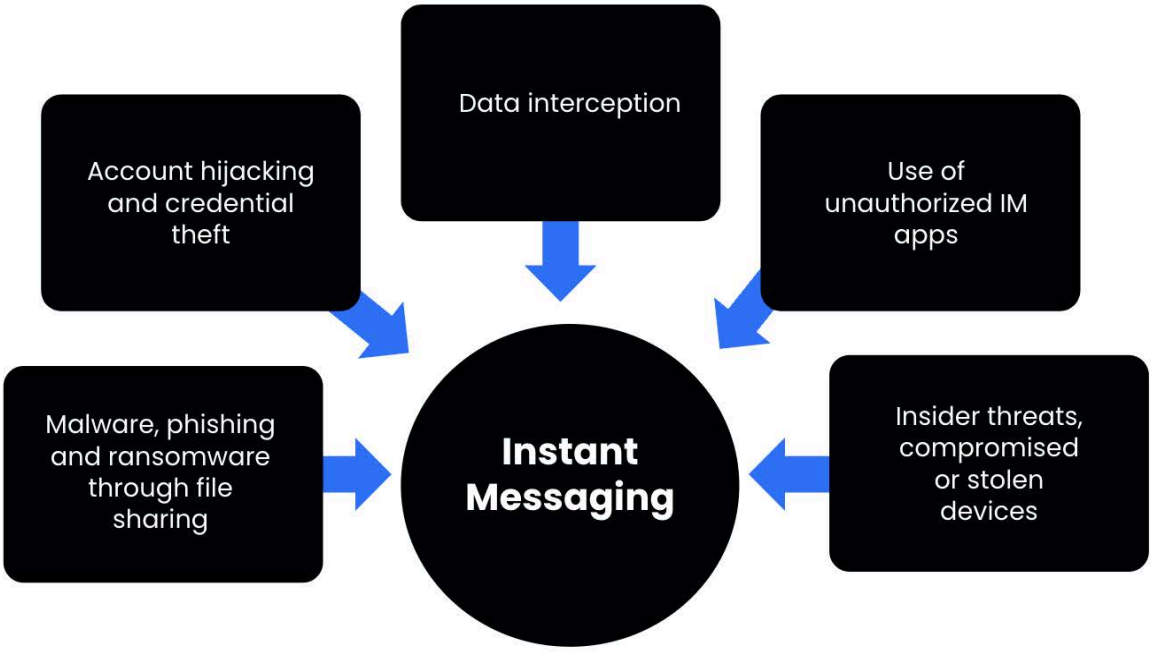
Critical sectors also utilize many interconnected cyber-physical systems, where sensors, robotics, and intelligent monitoring all interact with processes in the physical world. These systems, from water treatment and medical monitoring to smart energy grids, are often intricate and inseparable. Therefore, an attack on one critical sector could result in disruption to other critical sectors.

Cybersecurity and Instant Messaging

In today's hyperconnected business culture, data breaches, malware, and ransomware attacks can have a significant impact on the organization. Casually incorporating messaging platforms into the business adds to the security challenges. Messages are prone to interception if not properly secured, and credential theft allows attackers to access sensitive communications traversing these messaging platforms.

Workers often use multiple devices for business communications, including phones, laptops, tablets, and smart watches. Some devices are supplied by the organization, but increasingly employees are allowed (even encouraged) to use their personal devices for business communications. This "bring your own device" or BYOD model is driving the growing number of endpoints, raising significant security concerns while complicating the organization's information security system(s).

Moreover, different devices have varying security features, and older models may not support the latest updates. Devices may be lost or stolen, or simply not comply with an organization's current regulatory requirements.



This rise in messaging platforms for business communications, combined with the growth of BYOD as accepted information security practice, are accelerating the shift in cyber defense. Building (fire)walls around the business to keep out bad actors is giving way to a new approach: protecting access and identity through **access control** that leverages Zero Trust principles and stronger identity management.

This task is daunting; as new technologies are introduced, bad actors will seek to exploit them and develop new cyber threats targeting access and identity management protections.

One such emerging technology, quantum computing, promises to advance science and innovation across multiple industries. However, it also ushers in concerns of quantum-based decryption driven by the unique processing these quantum computers will be able to perform.

THE QUANTUM PARADOX

> "The disruptive potential of quantum technology will make the change of the Internet era look like a small bump in the road!"
>
> - **Kevin Coleman, Author and Thought Leader on Emerging Technologies**

> "When it becomes available, a [cryptanalytically relevant quantum computer] could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions."
>
> - **White House National Security Memorandum 10 May 4, 2022**

Support for quantum-based technologies is both effusive and cautious. On one hand, the promise of quantum computing for solving complex problems in critical sectors is inspiring. Quantum technology portends global advancements in human existence well beyond those derived from the silicon chip. However, lacking sufficient oversight, quantum computing advancements could be leveraged to disrupt essential communications, expose national secrets, and destroy protections required for the safe functioning of societies.

Offensive quantum computing

Developed as a theoretical construct in the 1980s and '90s, quantum computing has emerged over the last two decades as a viable yet experimental technology.

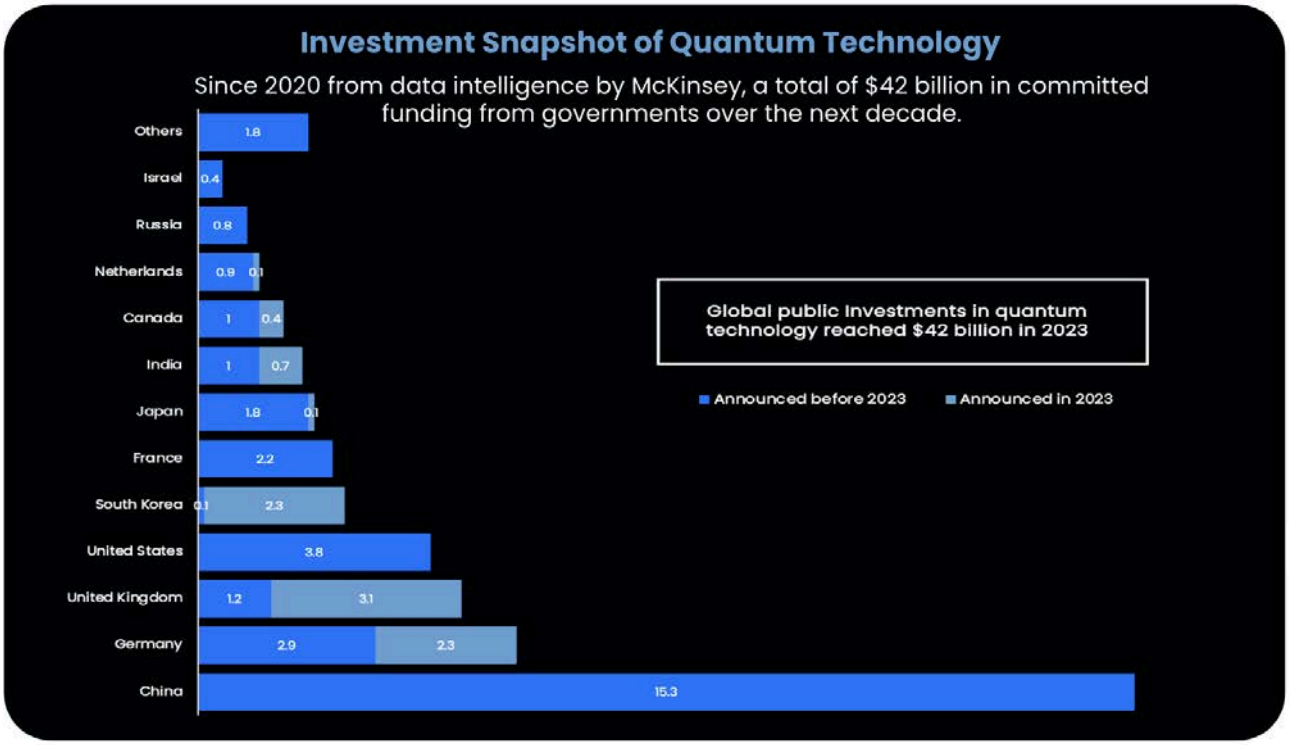
In simple terms, quantum computers attempt to take advantage of the unique properties of

matter and energy at the subatomic level–such as entanglement and superposition[1]–to deliver a new computing approach where the bits in classical computing are replaced with quantum bits or "qubits."

Despite technical challenges that must be overcome to achieve practical and scalable quantum computing, both theoretical and experimental evidence suggest that quantum computers could soon outperform classical systems in a variety of tasks.

Quantum computing holds great promise for innovation and transformational applications, from improving drug and material discovery to more efficient systems such as value chains and delivery networks. According to a 2024 McKinsey report[12], quantum computing could benefit four prominent sectors—chemicals, life sciences, finance, and mobility—to the tune of up to $2 trillion in economic growth by 2035.

The surge in private investment and government funding has significantly advanced quantum technology. Governments have established research centers dedicated to quantum technology, serving as focal points in the quantum ecosystem. These investments not only fuel the potential of quantum technologies but also amplify associated risks.



While according to Qureca[13], total capital to quantum technology is projected to be $104 billion by 2040.

[1]Core to quantum computation is the manipulation of particles' two quantum mechanical behaviors: 'entanglement' and 'superposition.' Entanglement allows particles to mirror their behavior, and superposition is their ability to portray multiple states until measured.

There are three general categories of defensive quantum computing:

1. Post-quantum cryptography (PQC).
2. Quantum key distribution (QKD).
3. Quantum random number generation (QRNG).

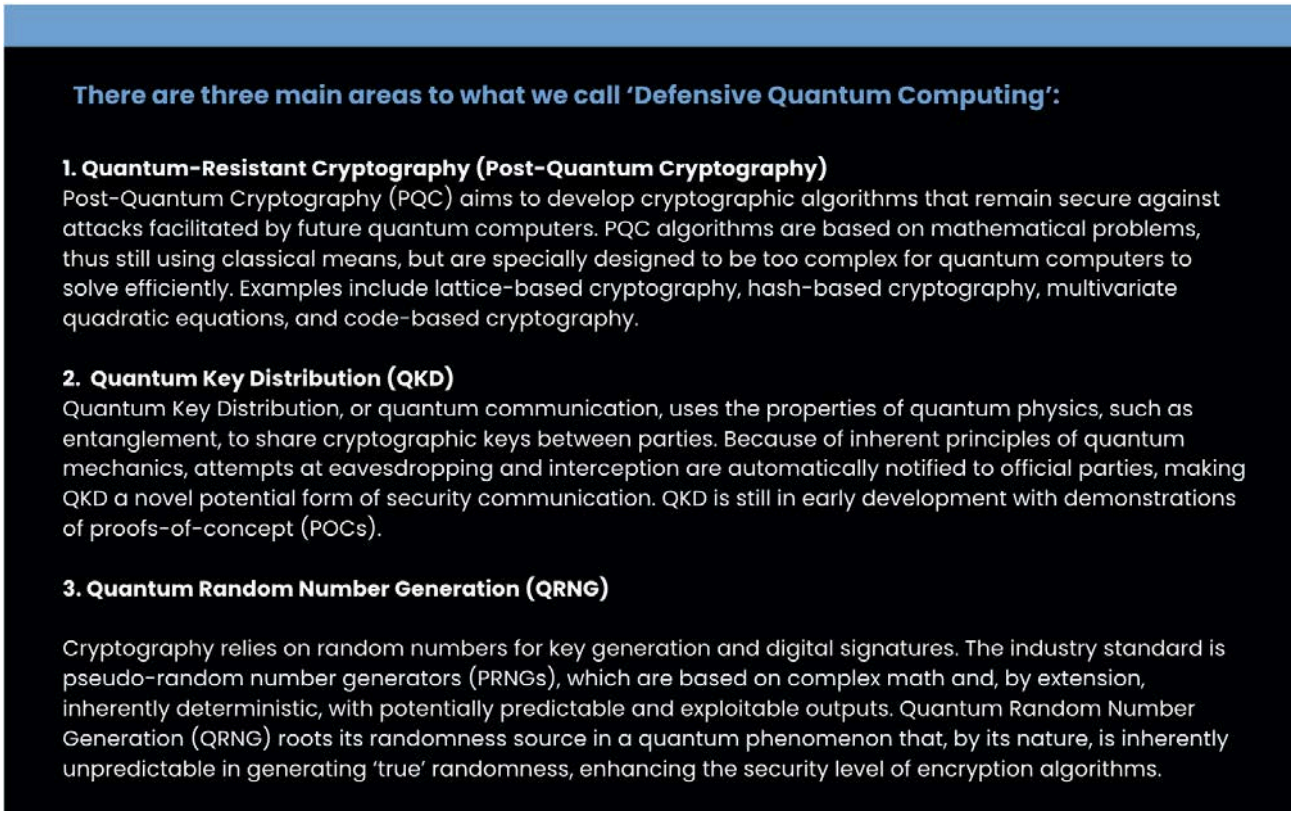
This paper addresses PQC.

Defensive quantum computing and PQC

Quantum computing's likely impact on classical encryption methods like RSA and ECC (Elliptic Curve Cryptography) relies on the difficulty of factoring large numbers or solving discrete logarithm problems. Breaking these public, asymmetric key encryption schemes is a practical impossibility for classical systems. However, quantum decryption may manage to uproot these standard encryption algorithms.

The security of systems employing RSA is based on the principle that while it is simple enough to multiply two very large prime numbers, it is exceedingly difficult to reverse, i.e., to factorize that number back into its prime components.

Depending on the size of the keys and the algorithm used, estimates range from hundreds to billions of years[14] for classical computing to break these asymmetric keys. This makes RSA and similar encryption methods practically unbreakable today, which is why these encryption schemes have proven valuable over the past forty years.



Factorization for large numbers using quantum computers and quantum algorithms – such as Shor's Algorithm – could be significantly faster than classical systems. Projections indicate that an adequately scaled and practically reliable quantum computer would need only a few hours[15] to break RSA encryption algorithms. And because so much of today's communications rely on RSA and similar encryption standards, the prospect of a quantum computer breaking these schemes presents a serious problem.

The Q-Day Menace

The day when quantum computers are large enough to break RSA and ECC cryptography is called "Q-Day."[16]

More of a milestone than a date, Q-Day signals the crossing of a computational "line in the sand" that current cryptographic algorithms have defended for over four decades.

There is much speculation regarding how long it will be before quantum computers are operational and sufficiently scaled to support a Q-Day attack. What is certain is that the pace of advancements in quantum computing technology is accelerating, shortening the Q-Day horizon.

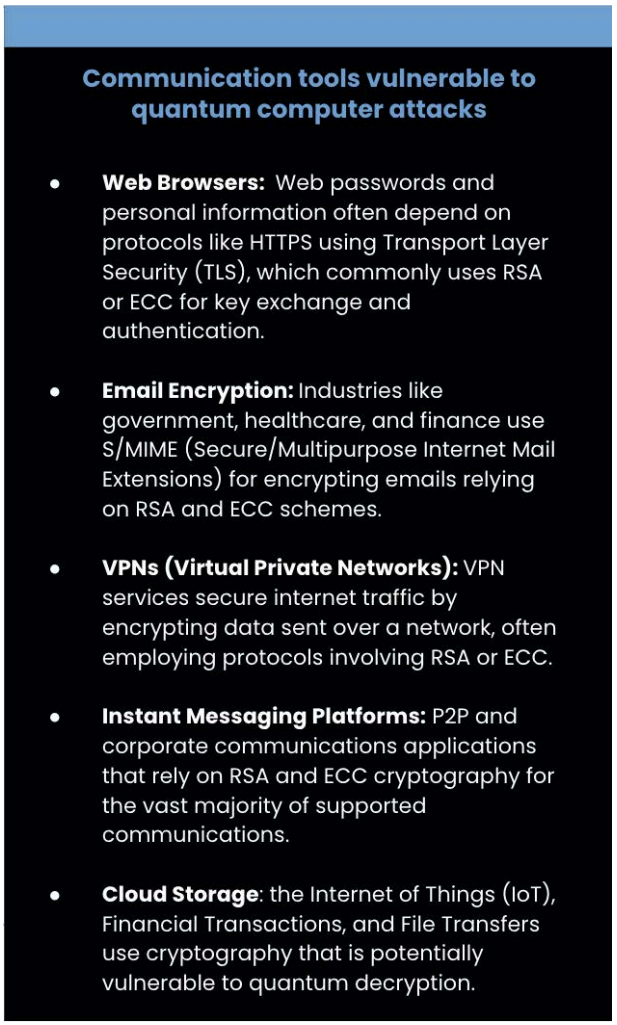
1980-90	1990-2010	2010 - Present	In Development
• Pioneers like Richard Feynman and David Deutsch establish the theoretical underpinnings for quantum computing	• Quantum algorithms such as Shor's and Grover's and quantum error-correcting codes discovered • First quantum logical gates created	• Quantum computers built with tens and 100s of qubits • Quantum advantage over classical computing proven for a select set of computations	• Widespread industry adoption of quantum computing for practical applications • Quantum computers able to break encryption systems

Quantum Computing Q-Day Timeline

Unlike classical bits, the qubits of quantum processors are extremely sensitive to interactions with their environments. On a high level, this is called noise, which results from unwanted interactions between qubits and their immediate and external environment, such as the surrounding materials and even Earth's electromagnetic field.

The conditions under which quantum computers operate must be tightly controlled to maintain qubit stability and prevent operational errors, i.e., noise mitigation (cleaning up the noisy qubit output). The larger the number of qubits, the greater the chance for instability and error. Taken together, the reliability and stability of qubits must increase with the number of qubits being utilized.

This is the dichotomy in quantum computation that error correction algorithms have mitigated. Although companies and state-sponsored research units invest billions of dollars annually to develop quantum technology to build more reliable systems, the creation of useful, fully error-corrected quantum computers has yet to arrive. Still, significant advances have been made in recent years. For example, in December 2023, IBM announced that it broke the 1,000-qubit barrier[17] with its Condor quantum computer.



Estimates vary as to the number of qubits needed to achieve Q-Day. In 2017, Microsoft Research published a paper[18] arguing that breaking ECC encryption would require about 2,500 qubits; while a 2020 study[19] by Craig Gidney and Martin Ekera proposed a method for factoring 2048-bit RSA integers requiring 20 million qubits. Credible projections suggest that cryptographically relevant quantum computers could arrive by this decade.

Two recent milestones suggest this timeframe. The first was in early 2024 when Microsoft and quantum computing company Quantinuum achieved over 14,000 experiments with no uncorrected error[20]. The other example published in Nature in late 2023 (between Harvard, QuEra Computing, MIT, and NIST/University of Maryland) presented a solution[21] based on a 'zone of entanglement' for qubits and a three-dimensional 'surface code' that ran 48 reliable qubits.

These achievements have prompted respectable institutions to flag cybersecurity professionals to prepare for Q-Day. A 2022 white paper from the World Economic Forum on transitioning to a quantum-safe economy stated that experts estimated Q-Day to be around 2032. Meanwhile, the 2023 Quantum Threat Timeline Report by the Global Risk Institute found that a surveyed group of 37 experts placed the time frame between 5 and 30 years[22].

The Q-Day conundrum

> "It is imperative for all organizations, especially critical infrastructure, to begin preparing now for migration to post-quantum cryptography."
>
> - **Jen Easterly, Director of the US Cybersecurity & Infrastructure Security Agency (CISA)**

Even with the uncertainty regarding a Q-Day timeline, there are several reasons for critical sector companies and organizations to take proactive measures today.

Preparing for quantum computing threats is a complex process. As the CISA, the NSA, and NIST outlined in their joint factsheet[23], organizations are tasked with establishing a "quantum-readiness roadmap" to plan the steps needed to protect their data.

Importantly, this roadmap starts with a complete **cryptographic inventory**, identifying how and where an organization uses cryptography, and assessing all quantum vulnerabilities.

Accelerated plan implementation then becomes an important consideration. The threat posed by quantum computing is of immediate concern due to ongoing **harvest now, decrypt later (HNDL)** cyber-attacks. In these scenarios, an attacker collects encrypted data to decrypt later when more powerful decryption tools, such as reliable quantum computation, are deployed. As quantum-safe technologies become more widely available, bad actors may accelerate their data capture activity before the sensitive information they seek can undergo quantum protection.

Data such as personally identifiable information (PII), trade secrets, and classified government information have longevity and must remain secure over long periods. The potential for future decryption means organizations must not only revise their protocols for data storage durations but, more importantly, begin transitioning to quantum-resistant encryption methods as soon as possible.

NIST and Post-Quantum Cryptography

Due to the HNDL threat and the urgency it imposes, groups worldwide, including NIST in the United States, have issued PQC standards. These standards involve cryptographic algorithms that can withstand attacks from quantum computers.

Launched in 2016, NIST's initiative, the PQC Standardization Process[24], involved soliciting, evaluating, and standardizing a set of quantum-resistant public key cryptographic algorithms. NIST has been working with the global cryptographic community to receive candidate algorithms and then subject them to evaluation for their security and performance.

After several rounds of selection and evaluation, in 2022, NIST identified four algorithms for standardization:

- For Public Key Encapsulation: (1) CRYSTALS-Kyber
- For Digital Signatures: (2) CRYSTALS-Dilithium, (3) FALCON, and (4) SPHINCS+

In August 2023, NIST released draft standards for all post-quantum cryptography algorithms except FALCON, then called for further public feedback and scrutiny on these drafts.

One year later, NIST announced the first three finalized PQC standards to protect critical digital infrastructure against quantum computer cyberattacks. Issued in the form of Federal Information Processing Standards (FIPS) for use by non-military government agencies and contractors, these final standards are described as:

FIPS 203 - ML-KEM (CRYSALS-Kyber)
FIPS 204- ML-DSA (CRYSTALS-Dilithium)
FIPS 205 SLH-DSA (SPHINCS+)

As NIST and related US public bodies work to establish tools for quantum-safe cryptography, critical sector organizations should proactively assess their security needs and begin implementing solutions to support their transition towards quantum-safe operations.

> "The transition to a secured quantum computing era is a long-term intensive community effort that will require extensive collaboration between government and industry. The key is to be on this journey today and not wait until the last minute."
>
> **- Rob Joyce, Director of NSA Cybersecurity**

Adapting to new technologies presents challenges for any organization, particularly those within the critical sector framework. Cost considerations and the complexities of implementing new systems are clear hurdles, and critical sector organizations typically move cautiously in response to new regulatory mandates.

Government bodies establishing specific guidelines and standards proscribe the approach that critical sector executives–tasked with migrating the organization to new security standards–must take. In the case of PQC mandates, allowing for sufficient planning and implementation, and considering the uncertainty around Q-Day timelines, regulators may establish compliance target dates with long lead times.

The unique threat posed by HNDL attacks necessitates that all organizations take deliberate and proactive measures today to ensure the protection of their data tomorrow. The long retention periods required for medical, financial, military, and governmental records alone are driving considerable activity toward the asset and systems inventory work described above. To date, few organizations are implementing quantum-safe technologies, leaving their data and conversations vulnerable to HNDL tactics from which they can never recover.

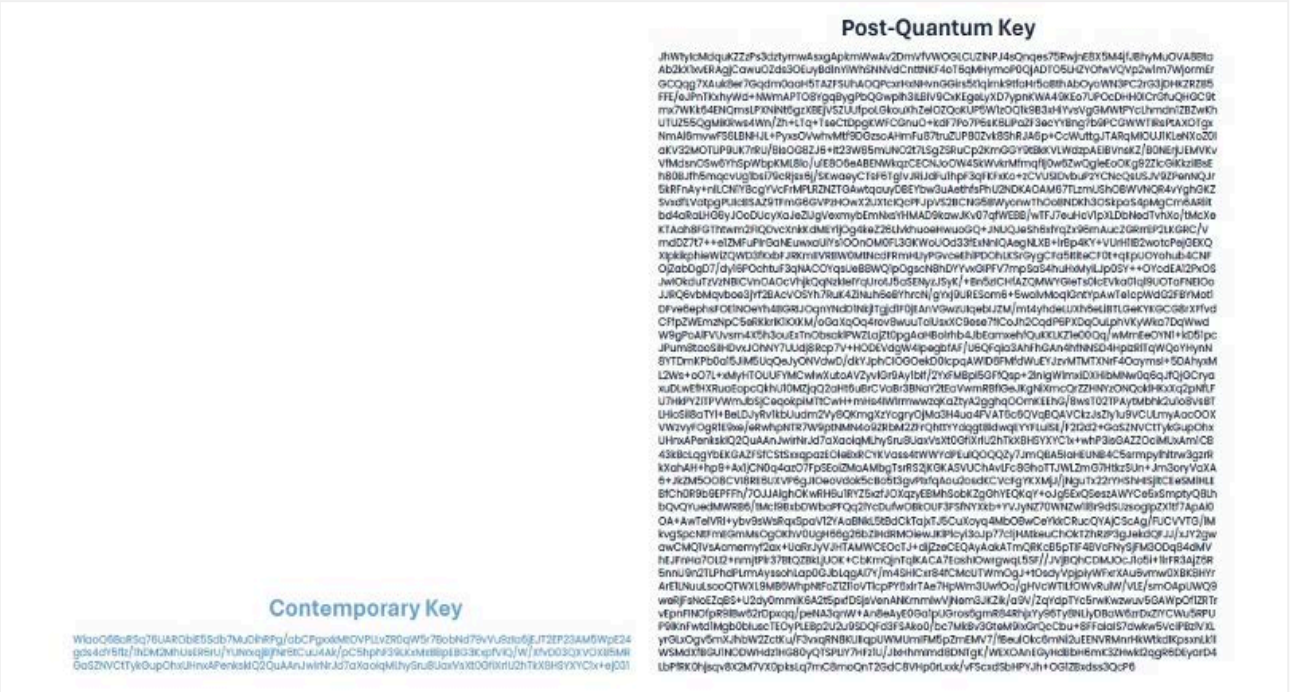
The limitations of PQS in instant messaging solutions

It is clear why there is such hesitation in migrating to PQC-enabled platforms. While straightforward in concept, the challenge of adopting PQC protection is daunting.

One major challenge is that PQC-generated keys are derived using highly complex mathematical processes, and involve operations using large matrices and vectors. These steps include matrix-vector multiplication (to mix public and secret information), modulo arithmetic (to keep values within certain limits and increase security), noise addition (to make it difficult to reverse the process), and polynomial arithmetic (to increase complexity).

As a result of these complex mathematical operations, PQC keys are as much as twelve (12) times larger than the keys generated by traditional encryption algorithms. This overhead becomes problematic for larger groups, forcing some messaging platforms to limit their deployment of PQC.

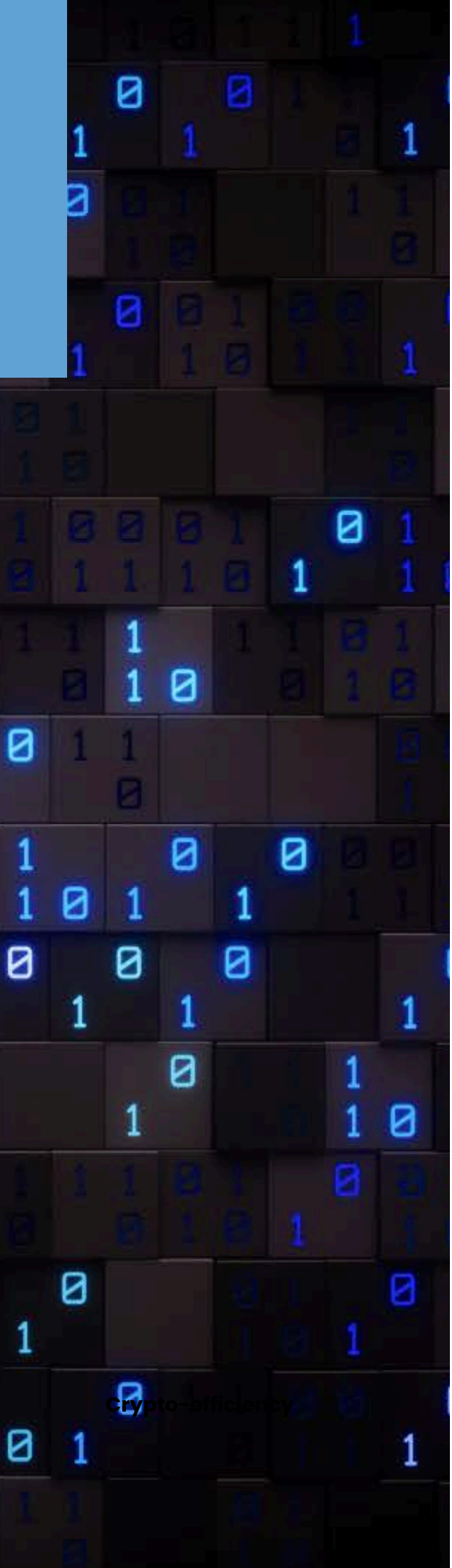
Quantum-resistant keys are 12x larger than current keys



A second challenge is that messaging platforms often lack crypto-agility[25]—the ability to switch easily between classical and quantum-resistant standards. The complex cryptographic components of today's digital systems can require extensive modifications to system architecture(s) to enable switching between classical and PQC security protocols.

ML-KEM algorithms create very large encryption keys; the message overhead resulting from these larger keys may be less significant for small groups, but it can be unwieldy for large organizations with thousands of users operating potentially tens of thousands of devices, all requiring constant safeguarding.

Fortunately, innovations in messaging security create a process for more efficient key distribution. One relatively recent innovation, Messaging Layer Security, provides a solution to overcome the challenges arising from the deployment of PQC.



MESSAGING LAYER SECURITY (MLS)

Transport Layer Security (TLS) is widely used to secure communications because it efficiently encrypts data from point to point. However, a major vulnerability of TLS is the potential for "man-in-the-middle" attacks.

In these attacks a threat actor can break the encryption and access all encrypted messages and files. That threat actor could, further, passively surveil the conversation(s) going forward for continued security compromise.

Organizations using instant messaging must be confident that their communication tools are providing the best security measures available. Innovative key distribution protocols have been developed by the IETF to provide additional safeguards for messaging and collaboration. One new protocol, called Messaging Layer Security, provides considerably more protection for messages and files.

The Efficacy of MLS

> "MLS provides unsurpassed security and privacy for users of group communications applications. Using MLS, participants always know which other members of a group will receive the messages they send, and the validity of new participants joining a group is verified by all the other participants."
>
> – **IETF press release[26], July 19, 2023**

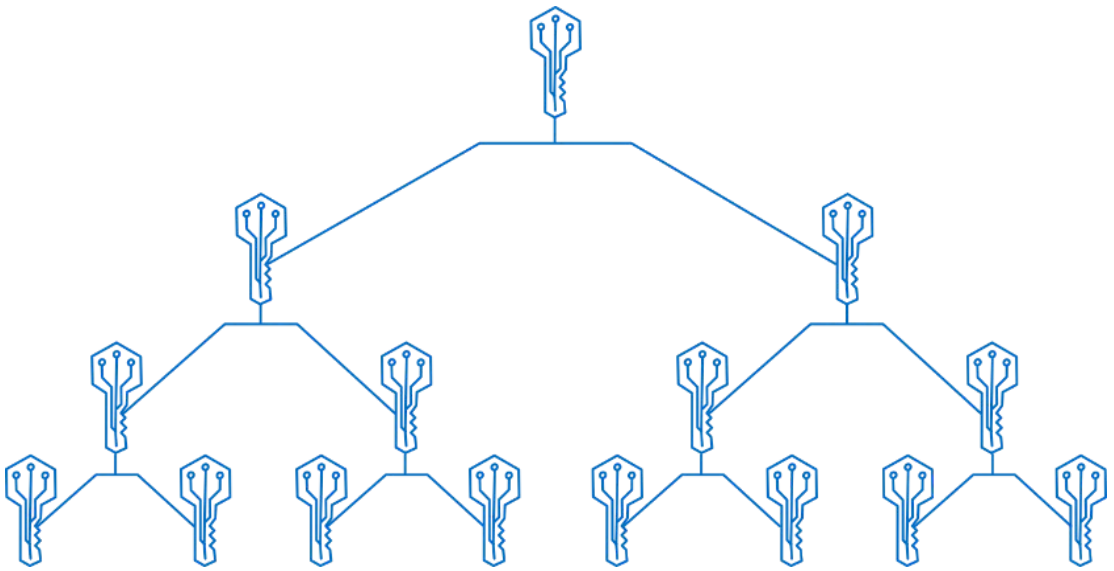
In July 2023, the IETF released the Messaging Layer Security protocol[27]. MLS ensures end-to-end security of a given message regardless of the number of intermediaries involved or where the data is stored. This way, MLS is independent of the security of the transport layer(s) being used. A bad actor that breaks the TLS encryption faces more encrypted data.

For critical sector organizations that require a very high level of security for partners, MLS ensures lower management of third-party security risks, as data protection for messages and files is provided throughout their in-transit and at-rest states.

Crypto-efficiency

MLS uses a tree-based approach to key management that is scalable for large groups. This efficiency of encryption key distribution is called crypto-efficiency.

GLYPH's ratchet tree



The benefit of Messaging Layer Security (MLS) for key distribution is that MLS scales in a logarithmic manner, whereas traditional key distribution mechanisms scale linearly. Unlike classical encryption, MLS has been designed specifically for group communications of any size, providing the security and efficiency that organizations require from modern messaging applications.

By way of illustration, imagine a channel in a messaging platform that accommodates 1,000 devices, traditional point-to-point solutions would require sending 999 unique keys to protect a conversation. In contrast, MLS would only require sharing of 10 keys.

The results get more dramatic for larger groups; for a group with 10,000 devices, a traditional solution would require sending 9,999 unique keys, whereas the MLS solution would need only 14 keys per device, resulting in much lower overhead for each message sent.

The inefficiency of classical protocols is why some secure messaging platforms revert to shared group keys, where group files and conversations are again subject to man-in-the-middle attacks.

Requirements for Quantum-Safe Collaboration

Much has yet to be determined about post-quantum cryptography and how organizations should best prepare for the quantum threat. Nevertheless, with decades of digital cryptography at risk, PQC-enabled messaging platforms need to be both cryptographically effective and supportive of digital communications.

The following list highlights basic security requirements for quantum-safe collaboration platforms:

Zero Trust Principles

Zero Trust security models rely on the principle of "never trust, always verify," meaning that all parties and devices attempting to access a given network—regardless of whether inside or outside the network's perimeter—must be authenticated and verified. Gartner projects that by 2026, 10% of enterprise companies[28] will have zero trust programs in place as opposed to just 1% as of 2023.

Multi-factor Authentication

Devices accessing the communications platform must have multi-factor authentication (MFA) capabilities in line with Zero Trust principles. This includes biometrics, UBI keys, authenticator software, and/or other trusted identity verification solutions. Robust, persistent presence and liveness-checking solutions further enhance the security of the messaging platform.

Frequent Key Rotation

The process of periodically changing cryptographic keys to limit the amount of data accessed if a key is compromised, reducing the risk of long-term key compromise. Public keys should be rotated whenever a new participant enters, leaves a group, or starts a new conversation.

Crypto-agility

A system's ability to quickly and adaptively switch between cryptographic algorithms and protocols will determine how well it can respond to emerging threats. Applications should be built with a framework that allows for different cryptographic libraries and algorithms to be plugged in as compliance standards evolve and new threats emerge.

Crypto-efficiency

Distributing large-size PQC keys via TLS-only solutions slows messaging performance, encumbers communications for large groups, and potentially compromises the real-time virtue of instant messaging that is critical to effective incident management. PQC key distribution should include appropriate protocols designed to handle quantum-safe keys for efficiency. However, organizations often prioritize agility over efficiency, despite all authorized devices participating in very large channels.

Modular Architecture

Fixed-architecture platforms can impose platform migration costs on organizations seeking to embrace new requirements and emerging technologies. These frequent migrations are resource-intensive, impeding workforce productivity. A modular architecture provides the flexibility and scalability to customize messaging solutions, while delivering futureproof protections to the organization.

The Glyph Protocol

SENTRIQS' developed the first messaging platform to offer both PQC and MLS. Specifically, SENTRIQS first deployed the MLS standard on its messaging platform in January of 2022 and then offered PQC with MLS on the platform shortly after NIST announced its PQC finalists in July of 2022. This PQC deployment included CRYSTALS-Kyber for public key generation and CRYSTALS-Dilithium for generating digital signature keys, both of which have been upgraded to the new FIPS 203 and FIPS 204 standards, respectively.

Dubbed the "GLYPH Protocol," this unique integration of MLS with PQC has been refined over the past two years to meet the real-world requirements of critical sector organizations.

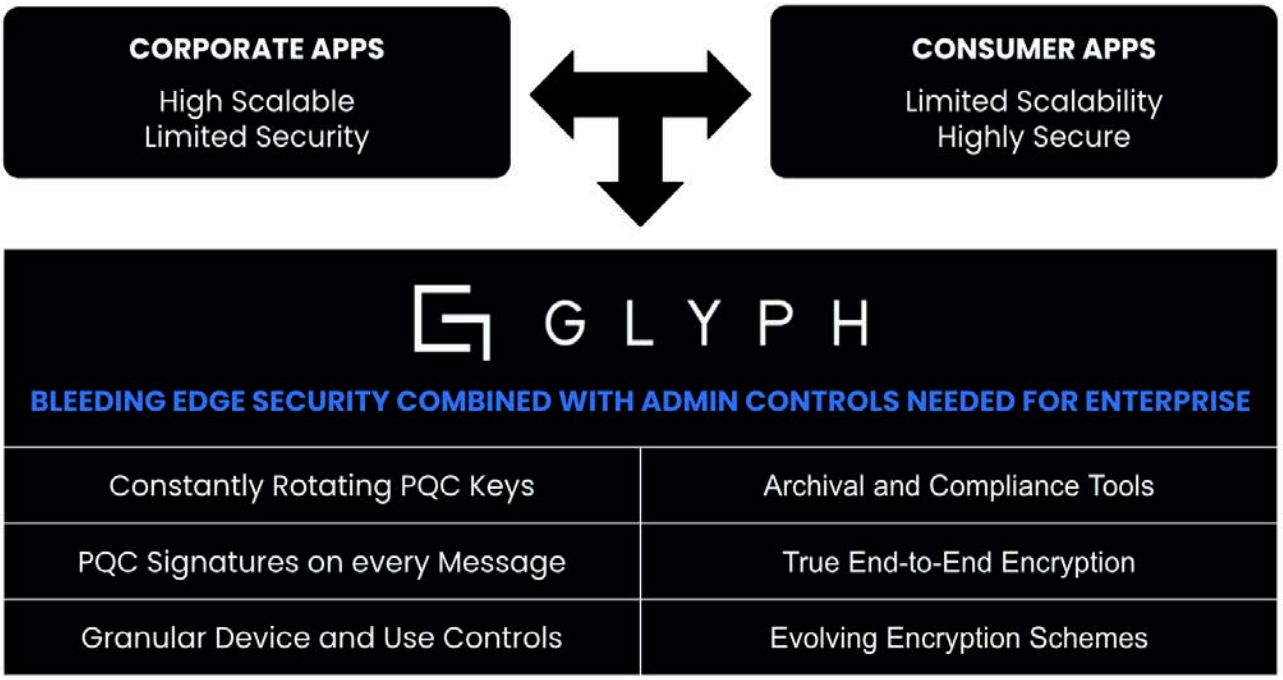
GLYPH – A Messaging App

Built on the GLYPH Protocol, GLYPH offers regulatory-compliant privacy and data protection, equipping teams with robust and adaptive collaboration capabilities.

GLYPH is a step up from classical messaging applications, which are limited in providing security for large groups due to inefficiency in encryption key management. Before GLYPH, organizations had to contend with two alternatives, neither of which are optimal:

- Enterprise-centric platforms that have robust collaboration features, but not the robust PQC security features that critical sector institutions will require going forward.

- Consumer-centric messaging apps that may provide some PQC protection for small groups, but are forced to revert to more vulnerable security methodologies for communications within large channels.



GLYPH offers the best of both approaches: security that is more robust than consumer-centric solutions, and efficiency that is as scalable as any enterprise-centric platform. A security heavyweight, GLYPH is built for critical sector organizations that rely on uncompromised security and real-time communications.

GLYPH allows administrators to choose a public key cryptography scheme for each workgroup they set up on the platform. With crypto-agility, users can choose between ML-KEM, providing NIST-approved quantum-resistant encryption, and a multi-layer hybrid PQC protocol that combines lattice-based protections with linear equation-centric algorithms (e.g HHL) for unmatched quantum protection.

GlyphKit – SDK and API Integrations

GlyphKit is a software development kit (SDK) and an API, available for iOS, Android, Windows, and the web, that allows third-party developers to incorporate the GLYPH Protocol into their software. GlyphKit's modular architecture offers developers the flexibility of incorporating any or all of SENTRIQS' MLS and PQC tools into their applications.

GlyphKit also provides cloud-based solutions that offer flexible deployment options, such as isolated on-premises systems or highly secure air-gapped networks, to meet stringent security and regulatory requirements.

Security without compromise

Critical sector institutions and the communities they serve depend on security systems that can meet current and future needs. This means, at a minimum, adopting collaboration solutions that provide crypto-agility and crypto-efficiency features to support the security and scalability of their communications.

With its modular architecture, GLYPH allows individual system components to be independently updated or replaced without significant end-user disruption or wholesale replacement.

GlyphKit extends these benefits to developers to avoid compromising when using their organization's preferred application(s). Productivity and operational software can be enhanced to include the ultra-secure messaging and collaboration features offered by the GLYPH Protocol.

13 GLYPH FEATURES

1. Modular Encryption Architecture: GLYPH is purpose-built to evolve as PQC develops. When technology emerges and new security and compliance protocols are established, GLYPH can be updated to give users the option of incorporating new security protocols, enabling crypto-agility.

2. Message Layer Security: SENTRIQS has combined the security afforded by the new MLS protocol for group messaging with PQC algorithms for quantum-safe messaging, a combination made possible only by a crypto-efficient and modular architecture. This combination is found nowhere else.

3. Digital Signatures: MLS gives GLYPH users the security of implementing digital signatures on every message in a group chat, ensuring the authenticity and integrity of communications and protecting against impersonation and tampering without high computational overhead.

4. Rapid Onboarding: Organizations and teams do not need any dedicated hardware, such as in-house or third-party servers, to add GLYPH to their operations, accelerating onboarding and lessening operational complexity and costs. GLYPH, further, has mass-onboarding capabilities and is platform-agnostic, enabling teams to use any device and operating system, giving them the flexibility to work securely and productively.

5. Multi-factor Authentication: GLYPH permits robust MFA options for access to secure workspaces, including biometric, UBI keys, authenticator software, and/or other trusted identity verification solutions. Persistent presence and living verification solutions are on the product roadmap.

6. Quantum-Safe Archiving: For compliance and due diligence purposes, administrators can store individual messages or conversation threads locally on a device with a dedicated crypto-agile private key instead of on third-party servers. This ensures in-house sensitive data ownership and privacy while lessening third-party complexity and cost. GLPYH's core crypto-efficiency and modularity architecture is the driver behind slimming cryptographic keys by 12 times for private archiving, responsiveness, quantum safety, and general lower computational load.

7. Group-Level Device Controls: GLYPH offers the granular control needed for hyper-secure networks. Administrators can make quantum-safe groups, change the security settings for each group, and toggle between PQC algorithms to fit different compliance requirements and security needs.

8. Post-Compromise Security: Post-compromise security (PCS) focuses on ensuring the security of a communication system in the event of compromise. This prevents bad actors from achieving man-in-the-middle attack to access data and passively surveille future conversations. GLYPH limits the damage caused by a compromise, and enables the system to recover and secure itself rapidly against further attacks.

9. Perfect Forward Secrecy: Perfect Forward Secrecy (PFS) ensures that even if attackers manage to compromise encrypted conversations, they cannot decrypt past communications, making all previous messages unavailable. GLYPH delivers PFS by generating unique session keys used only for the duration of each communication session and discarding them after the session ends.

10. Closed Ecosystem: GLYPH offers a closed and protected ecosystem where only permitted users and guests can participate. Administrators can restrict and manage groups, users, and interactions with the platform, and only approved applications, services, and integrations are allowed to interact with the platform. This minimizes the risk, for example, of introducing vulnerabilities through unvetted third-party software.

11. Rotating Secure Keys: With MLS, GLYPH rotates encrypted keys with every message, file, and activity, giving users increased security through GLYPH's industry-first combination of MLS and PQC. GLYPH ensures that only clients—not third-parties—have access to encryption keys. This means data can only be decrypted by the intended message recipient's device. Even in case of compromise, the data remains secure because encryption keys are not stored on the platform's servers.

12. Self-Healing: With transport-layer security, group dynamics are difficult to manage, maintain, and secure. GLYPH's modular and crypto-efficient architecture is self-healing, meaning if a participant exists in a group, all keys are refreshed, and security clearance is for group members only.

13. Remote Burn: Because data is stored on devices, not servers with a dedicated crypto-agile encryption key, GLYPH administrators can trigger remote burns to erase data in the case of a lost or compromised device, irrespective of the operating system, allowing for an immediate threat response to security threats.

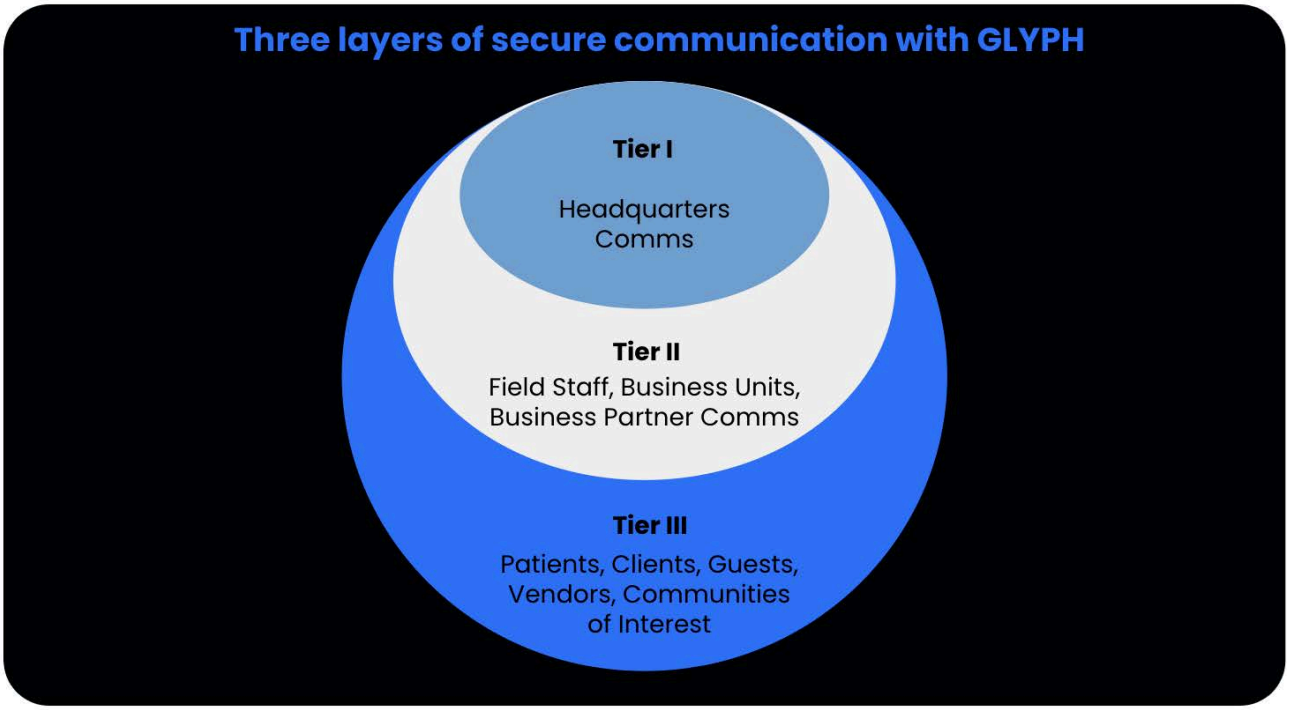
USE CASES

GLYPH lets customer organizations establish workspaces based on Zero Trust principles, allowing those customers to control what information can be shared with which authorized contacts (and on which devices) per workspace. This allows organizations to establish roles and responsibilities for several user categories based on the required access per group.

The use cases vary by industry and organizational requirements, but they all tend to fall within a general framework that involves three levels of segmentation.

For illustrative purposes, these are conceptualized as three rings of communication:

1. Inner Ring: executive staff / command staff at headquarters.
2. Middle Ring: field staff / remote employees.
3. Outer Ring: external parties, including clients, partners, vendors, community leaders, etc.



In public safety, for example, GLYPH protects communications for command staff at police headquarters in the inner ring, police officers in the middle ring, and local businesses and community leaders in the outer ring. For a financial institution, it might be executive staff in the inner ring, branch offices in the middle ring, and clients, vendors, and regulators in the outer ring.

Below are examples of industry-specific use cases.

Defense Industrial Base

THE CHALLENGE

The growing quantum threat poses a significant risk to the defense sector. Quantum computers could break standard encryption algorithms used throughout defense and national security communications in the exchange of intelligence data and classified information. Security breaches and vulnerabilities are matters of national security.

The defense industry relies heavily on secure third-party partners across supply chains and contractors, each of which could be disrupted by quantum-powered devices, leading to sabotage and downtime of operational activities, or theft of sensitive information via HDNL attacks.

THE SOLUTION

GLYPH gives military organizations the ability to deploy post-quantum cryptography to protect communications and activities against current and future threats. The defense sector can tap into the benefits of instant messaging while experiencing the performance benefits of crypto-efficient key distribution. Administrators and group owners can choose who can participate in group conversations and which particular devices they can use for a conversation, thereby reducing the need for third-party security management.

Emergency Services

THE CHALLENGE

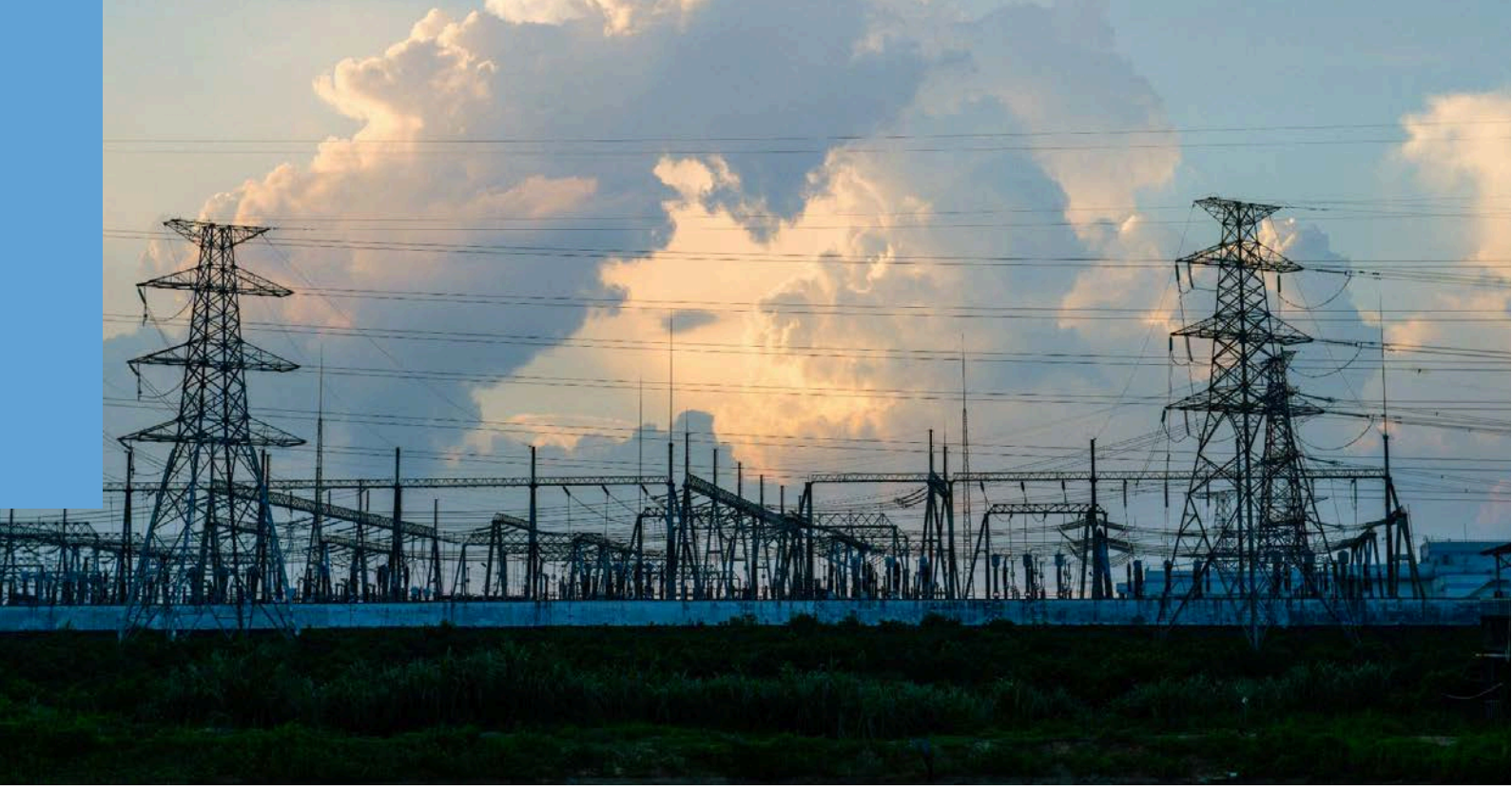
Emergency services, including police, fire, and medical response teams, rely heavily on secure, reliable, and instant communication networks to coordinate efforts in situations where responses within minutes can dictate the outcome between life and death. One challenge is managing the disparate communication and collaboration tools that span jurisdictions and communication platforms, while supporting stakeholders with varying degrees of authority and security clearance.

Further, malicious actors can target sensitive information databases such as police archives or medical records through HNDL attacks.

THE SOLUTION

GLYPH's quantum-safe messaging platform allows rapid primary and/or out-of-band (OOB) communications for organized, prioritized communications. Operating on public and/or private networks, this highly secure platform allows easy messaging and file sharing, with secure voice and video calling available with the push of a button.

GLYPH includes a Broadcast message feature so only designated users can post content to other members. When combined with GLYPH's unique Submission message group – where any participant can post a message or file, but only designated administrators can view that information – you have a powerful process to ensure that two-way information sharing is quick and easy, all without the constant distraction of submission notifications.



Utility Sector

THE CHALLENGE

The nation's water, gas and power facilities present highly vulnerable targets for bad actors. Compromised communications can expose potential attack vectors against these critical infrastructures, while harvested information can be stored for later decryption using quantum-based hacking techniques. Exposed assets can include shared files, intra- and inter-utility communications, operational plans, customer and supplier data, and financial information. By their very nature, public utilities and regulated monopolies lack robust alternative infrastructure, so operational impediments have immediate and widespread consequences that can dramatically impact entire communities.

Incident response teams must be careful while sharing information during suspected breaches, since hackers could be monitoring communications from inside compromised communication platforms. Even leaked communications regarding early suspicions could needlessly alarm other utilities and/or the community, and inhibit potential response options.

THE SOLUTION

GLYPH provides quantum-safe, end-to-end encrypted messaging, file sharing and video conferencing for secure incident response collaboration. The GLYPH platform uses Zero Trust principles, ensuring only authorized contacts can access proprietary information and join protected conversations. GLYPH lets utilities create individual workspaces to control access within each utility-managed environment, while permitting cross-workspace engagement through clearly defined participant roles.

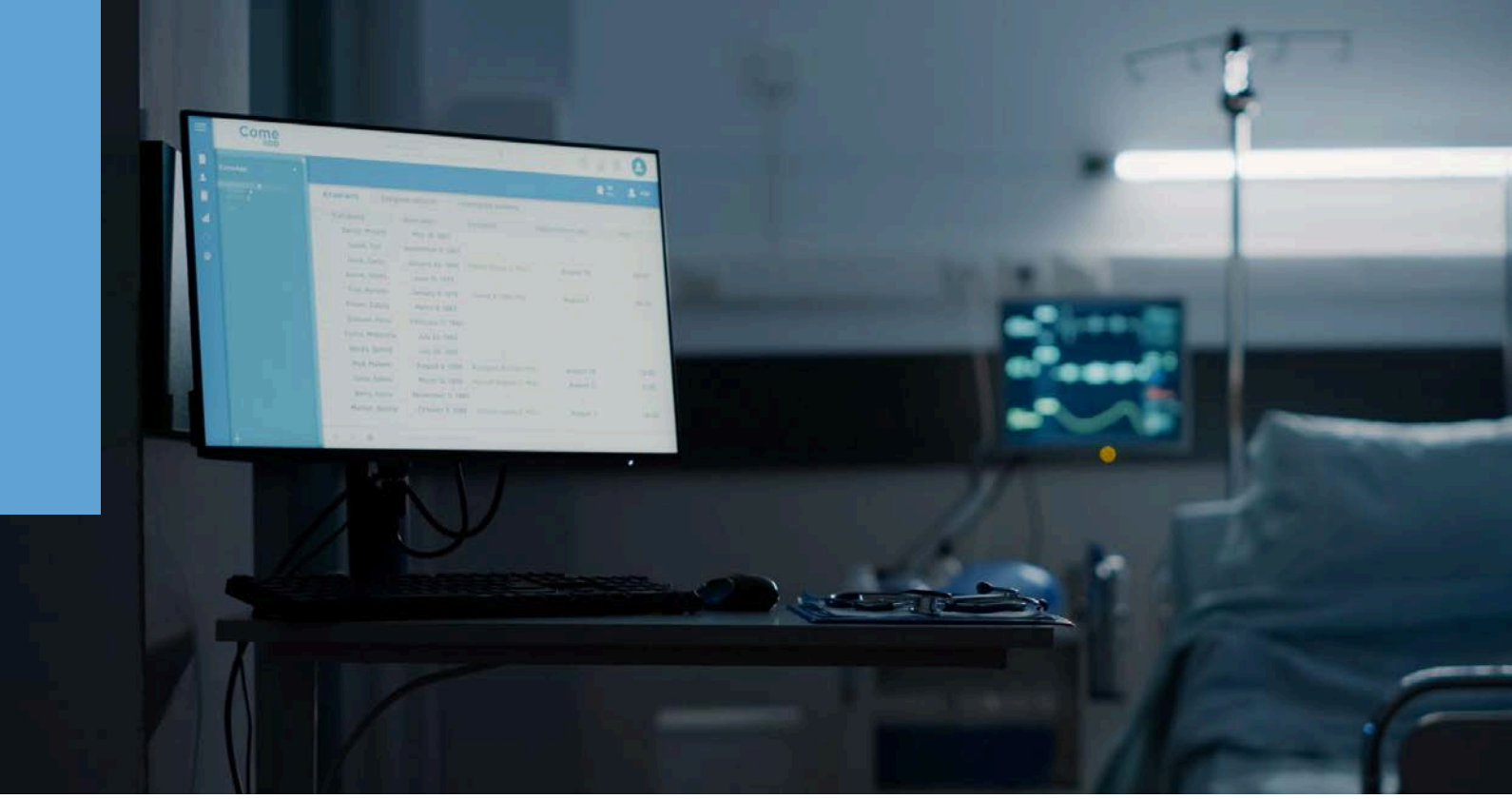
Financial Services

THE CHALLENGE

Financial institutions are under tremendous pressure to provide rapid access to real-time information while simultaneously ensuring that privileged data and conversations remain confidential, secure and documented. In an industry where timely information can generate astronomical rewards, and delayed responses can prove financially devastating, even occasional communication shortcuts can result in massive fines, damage to reputations, and loss of future business. Threats from cyber espionage increasingly heighten exposure for investment bankers and their firms, while quantum computers portend wholesale disruption to existing encryption protocols.

THE SOLUTION

With GLYPH, financial services users get PQC-enabled messaging for quick decision-making. The platform delivers unmatched privacy when communicating with clients, colleagues, staff, and partners. Clients and advisors can use their personal devices (phones, tablets, laptops, etc.) on public networks without compromising privacy or security. Collaboration options allow for on-demand secure video huddles, unlimited file size transfers, and automatic archiving of files and messages.



Healthcare & Public Health

THE CHALLENGE

Medical offices using classical social media platforms for office communications risk exposing confidential patient information during discussions with patients and other medical providers. These potential breaches destroy patient trust and risk violations of HIPAA regulations. While the growing practice of remote patient consultations has amplified compliance concerns, the advent of quantum computing puts historical and future patient health information (PHI) at even greater risk due to the limitations classical encryption technologies offer against future quantum-computing-enabled attacks.

Further, the prospect of HNDL attacks threatens healthcare institutions' reliance on industry-standard encryption algorithms such as elliptic curve cryptography, which could be undermined by quantum computing.

THE SOLUTION

GLYPH's messaging-layer security keeps every instant message encrypted with a dedicated key, giving healthcare professionals unmatched privacy for their communications. Patients can use their personal devices (phones, tablets, laptops, etc.) on public networks without compromising privacy. Equally empowering, doctors can now conduct vital patient consultations securely from their home offices, unlocking the full potential of robust remote health care. Public health officials can conduct virtual meetings and chats with confidence that their activities will remain compliant with current and future security standards.

Mineral Extraction

THE CHALLENGE

The battlegrounds for industries like mining and oil & gas can be cutthroat, with profits at stake in the race to seize prime development sites. With so much risk associated with site selection, mineral extraction companies pour massive resources into researching and evaluating the potential value of tracts globally. Amidst this high-stakes environment, the looming threat of corporate espionage is more imminent than ever.

Companies occasionally identify promising sites, only to witness a swift takeover of these assets just before they can make a move. Combatting these communications vulnerabilities includes fortifying internal communications between corporate management and the R&D team, and tightening control over access to critical R&D findings. The looming specter of quantum computing further heightens the urgency, as these machines pose a grave risk of breaking most encryption models.

THE SOLUTION

GLYPH provides end-to-end encrypted messaging, file sharing, and video conferencing for quantum-safe business collaboration. The GLYPH platform facilitates Zero Trust participation, ensuring only authorized contacts can access proprietary information and participate in confidential business communications.

SENTRIQS

WHO IS SENTRIQS?

Our guiding principle is 'security without compromise.'

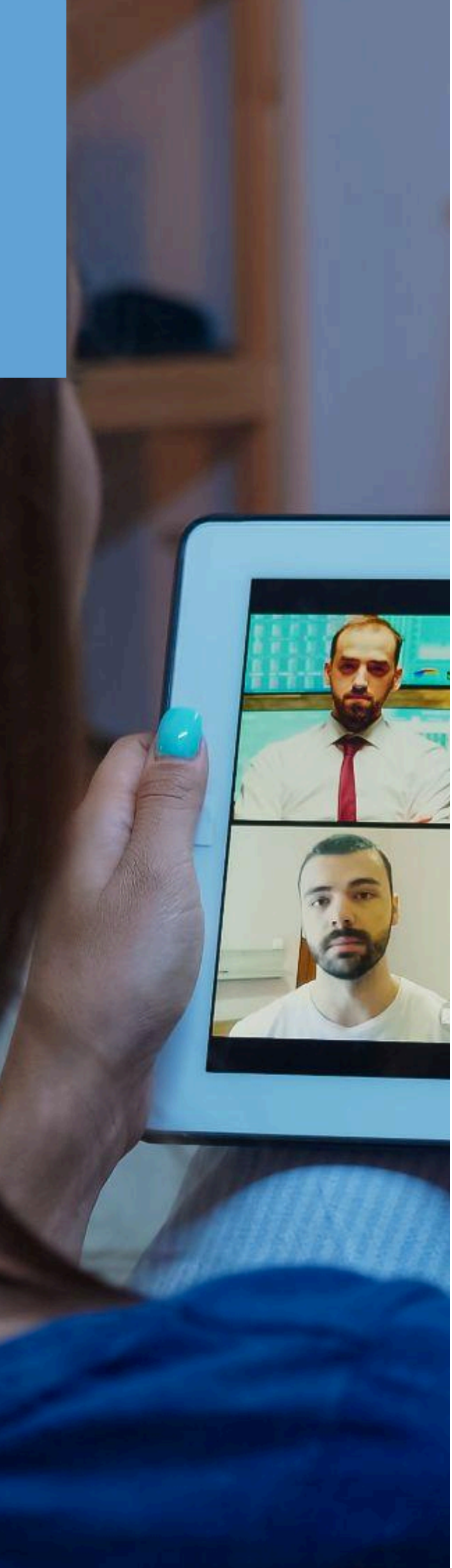
We make ultra-secure, flexible, and efficient messaging and collaboration tools for critical sector organizations, with a mission to ensure trust in the digital world. Security is our foundation, not a feature to be bolted on when required.

Technology evolves fast. Governments and regulators frequently call upon critical sector companies to act on new and developing security standards. Critical sector organizations, therefore, often are early movers in piloting cybersecurity solutions to meet the changing threat landscape from emerging technologies such as Generative AI for identity fraud, or quantum decryption through 'Harvest Now–Decrypt Later' attacks.

In a nutshell

GLYPH leverages a new Messaging-Layer Security (MLS) technology in a modular and crypto-efficient architecture that enables dynamic toggling between security standards, a process called crypto-agility.

Cyber-attacks are growing in frequency, sophistication, and impact, often targeting critical sectors due to the significant negative ramifications of operational downtime. Through implementing the post-quantum cryptography standards ML-KEM and ML-DSA, GLYPH gives organizations the confidence to carry out operations rapidly and dynamically, knowing that security measures are in place to shield their data and conversations from current and future threats.



CONCLUSION

Messaging platforms have shown themselves to be vital additions to the array of communication tools for broadly-defined critical sector organizations.

As remote workers and an increasingly mobile workforce drive messaging and collaboration application usage for business communications, these critical sector organizations experience improved employee effectiveness, responsiveness, and engagement.

However, harvest now, decrypt later (HNDL) attacks on critical sector organizations by bad actors are underway, and are expected to increase as quantum-safe technologies gain greater visibility.

The evolving cyber threat of quantum computing is real, and governments are taking determined steps to issue standards for post-quantum cryptography to replace many of the encryption protocols currently in use.

With NIST approving the first three protocols for post-quantum cryptography, cryptographic security has been bolstered.

The significantly larger size of PQC keys, combined with the limitations of key distribution architectures of classical messaging platforms, are forcing organizations to compromise on their future security.

The GLYPH Protocol was specifically engineered to deliver quantum-safe

crypto-agile and crypto-efficient collaboration tools to military, commercial and government organizations.

The GLYPH Protocol is available as a messaging app (GLYPH), and via a software development kit (GlyphKit) for quantum-safe communications today and tomorrow.

ABOUT SENTRIQS

SENTRIQS is a technology-pioneering company dedicated to developing advanced secure collaboration solutions. With a focus on cutting-edge cryptography and user-centric design, SENTRIQS empowers organizations to protect their most sensitive information into the quantum age.

For additional information or a demonstration of the GLYPH platform, visit sentriqs.com.

Endnotes

The definition of critical sectors where aggregated from officially listed critical infrastructure sectors from the following seven countries:

- The US: The Cybersecurity and Infrastructure Security Agency (CISA)
- Canada: Royal Canadian Mounted Police
- The EU: European Commission
- The UK: National Protective Security Authority
- Australia: Australian Government Department of Home Affairs
- Japan: The Japenese parlament called in English, 'the Diet'
- South Korea: The Committee for the Protection of Information and Communications Infrastructure

References

[1] Envoy, Hanover Research. ENVOY REPORT: Without accurate data, the physical workplace won't survive. Https://Envoy.com/: Envoy; 2023.

[2] McKinsey Global Institute. How hybrid work has changed the way people work, live, and shop. Https://Www.mckinsey.com/Mgi: McKinsey Global Institute; 2023.

[3] Mugayar-Baldocchi M, Schaninger B, Sharma K. The future of the workplace: Embracing change and fostering connectivity. Back to People & Organization Blog - Our Insights 2021. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-organization-blog/the-future-of-the-workplace-embracing-change-and-fostering-connectivity (accessed October 8, 2024).

[4] Cybersecurity and Infrastructure Security Agency. Critical infrastructure sectors. Cybersecurity and Infrastructure Security Agency 2022. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (accessed October 8, 2024).

[5] Royal Canadian Mounted Police. Safeguarding critical infrastructure. Royal Canadian Mounted Police 2024. https://rcmp.ca/en/federal-policing/national-security/safeguarding-critical-infrastructure (accessed October 8, 2024).

[6] European Commission. Critical infrastructure resilience at EU-level. Migration and Home Affairs 2023. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-ra

dicalisation/protection/critical-infrastructure-resilience-eu-level_en (accessed October 8, 2024).

[7] National Protective Security Authority. Critical National Infrastructure | NPSA. Wwwnpsagovuk 2023. https://www.npsa.gov.uk/critical-national-infrastructure-0 (accessed October 8, 2024).

[8] Australian Government - Department of Home Affairs. Protecting Critical Infrastructure and Systems of National Significance. Wwwhomeaffairsgovau 2020. https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems (accessed October 8, 2024).

[9] NEC Corporate Marketing Group. Safter Cities & Public Services: Commercial facilities as targets: New threats to critical infrastructure. Https://Sg.nec.com/: NEC; 2025.

[10] Fraunhofer. Critical Infrastructure Sector. CIPedia 2024.

[11] Rabinowitz H, Lyngaas S. FBI director will deliver stark warning on Chinese hackers in remarks to House panel | CNN Politics. CNN Politics 2024. https://edition.cnn.com/2024/01/31/politics/china-hacking-infrascture-fbi-director-christopher-wray/index.html (accessed October 8, 2024).

[12] McKinsey Digital. Steady progress in approaching the quantum advantage. Https://Www.mckinsey.com/Capabilities/Mckinsey-Digital/How-We-Help-Clients: McKinsey Digital; 2024.

[13] Kaur M. Overview of Quantum Initiatives Worldwide 2023 1202. https://www.qureca.com/overview-of-quantum-initiatives-worldwide-2023/ (accessed October 8, 2024).

[14] Vaishnavi A, Pillai S. Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods. Journal of Physics: Conference Series 2021;1964:042002. https://doi.org/10.1088/1742-6596/1964/4/042002.

[15] Emerging Technology from the arXivarchive page, MIT Technology Review. How a quantum computer could break 2048-bit RSA encryption in 8 hours. Computing 2019. https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/ (accessed October 8, 2024).

[16] Fernandez R. Is Q-Day — The Day Quantum Computing Hacks Everything — Approaching? Techopedia - Cybersecurity - Cyber Threats 2024.

https://www.techopedia.com/q-day-is-coming-how-experts-secure-quantum-computing (accessed October 8, 2024).

[17] Gambetta J. The hardware and software for the era of quantum utility is here. IBM Quantum Blog 2023. https://www.ibm.com/quantum/blog/quantum-roadmap-2033 (accessed October 8, 2024).

[18] Roetteler M, Naehrig M, Svore KM, Lauter K. Quantum resource estimates for computing elliptic curve discrete logarithms. ArXivorg 2017. https://doi.org/10.48550/arXiv.1706.06752.

[19] Gidney C, Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum 2021;5:433. https://doi.org/10.22331/q-2021-04-15-433.

[20] Swayne M. Beyond NISQ: Microsoft And Quantinuum Research Project Yields "Most Reliable Logical Qubits Ever Recorded." The Quantum Insider - Research - Quantum Computing Business 2024. https://thequantuminsider.com/2024/04/03/beyond-nisq-microsoft-and-quantinuum-research-project-yields-most-reliable-logical-qubits-ever-recorded/ (accessed October 8, 2024).

[21] Swayne M. TQI Exclusive: Harvard and QuEra Scientists Say Shuttling Qubits, Parallelism May Power the Ride to Practical Quantum Computing. The Quantum Insider - Exclusives 2024. https://thequantuminsider.com/2024/01/12/tqi-exclusive-harvard-and-quera-scientists-say-shuttling-qubits-parallelism-may-power-the-ride-to-practical-quantum-computing/ (accessed October 8, 2024).

[22] Mosca DrM, Piani DrM, Global Risk Institute, evolutionQ Inc. 2023 Quantum Threat Timeline Report. Https://Globalriskinstitute.org/: Global Risk Institute; 2023.

[23] Cybersecurity & Infrastructure Security Agency, National Security Agency - United States of America, National Institute of Standards and Technology - U.S. Department of Commerce. QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY. Https://Www.cisa.gov/: Cybersecurity & Infrastructure Security Agency; 2023.

[24] NIST: Computer Security Resource Center (CSRC). Post-Quantum Cryptography Standardization. CSRC | NIST 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization (accessed October 8, 2024).

[25] Barker W, Polk W, Souppaya M. Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum

Cryptographic Algorithms. Https://Www.nist.gov/: NIST: U.S. Department of Commerce; 2021.

[26] IETF News. New MLS protocol provides groups better and more efficient security at Internet scale. Https://Wwwietforg/ 2023. https://www.ietf.org/blog/mls-protocol-published/ (accessed October 8, 2024).

[27] Barnes R, Beurdouche B, Robert R, Millican J, Omara E, Cohn-Gordon K. RFC 9420 The Messaging Layer Security (MLS) Protocol. Https://Www.rfc-Editor.org: RFC Editor; 2023.

[28] Keen E. Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024. Gartner Press Release Newsroom 2023. https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024 (accessed October 8, 202

SENTRIQS