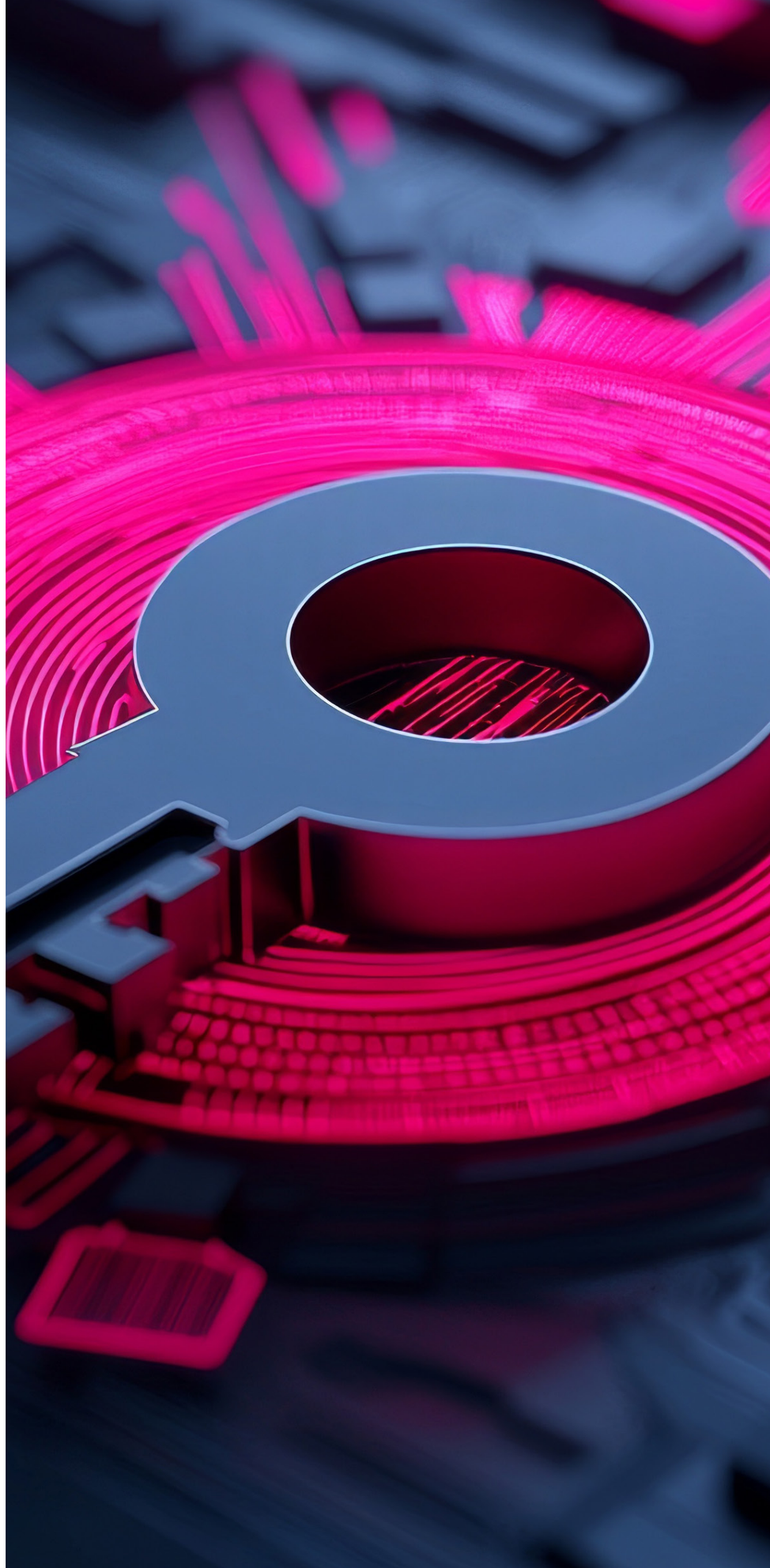
ECHOWORX™

IT PAYS TO BE SECURE

Echoworx Prepares for Quantum Computing



Introduction

As quantum computing advances, encryption faces new vulnerabilities, pushing organizations to adopt **post-quantum cryptography (PQC)**. PQC involves algorithms designed to withstand attacks from quantum and classical computers alike. Echoworx recognizes the risks posed by quantum threats and is proactively implementing measures to secure cryptographic keys against potential breaches.

Here’s a summary of our efforts to stay ahead in safeguarding encryption.

Table of Contents

Understand the Quantum Threat

Current Vulnerabilities

Algorithms like RSA, ECC, and DSA face serious exposure to quantum algorithms like Shor's, which can efficiently crack large-number factoring and discrete logarithms.

While large-scale quantum computers are still a decade or two away, the clock is ticking.

The risk of "**Harvest Now, Decrypt Later**" is real.

Encrypted data, particularly emails in transit over TLS, could be intercepted today and decrypted once quantum computing matures, exposing sensitive information.

The window to prepare is narrowing.

Migrating to quantum-resistant algorithms isn't an overnight process—it requires foresight, planning, and execution. Failure to act now could leave organizations scrambling to adapt when the quantum era arrives.

Assess Current Cryptographic Systems

Inventory Encryption Usage

Identify where cryptographic algorithms are applied, such as in data storage, communications, and authentication.

Echoworx uses AES keys (quantum resistant) with AWS KMS, so the persisted data is stored in a quantum resistant manner. S/MIME keys, PGP private keys, PDF passwords, and portal messages are all persisted encrypted with AES encryption without any PKI.

That said, certain areas remain vulnerable to quantum-based threats.

For instance, portal messages use PKI as part of the Encrypted Mail Gateway for message exchange, leaving communications recorded by an attacker potentially susceptible to future quantum decryption. While this risk is mitigated by the similarly vulnerable TLS protocols used to send messages, the absence of standardized quantum-resistant TLS solutions means there's no immediate fix.

Echoworx is closely monitoring developments in post-quantum standards and plans to adopt widely supported solutions as they emerge.

AWS has introduced a hybrid post-quantum TLS protocol for KMS API calls as a defense against potential attacks where encrypted communications are stored and later decrypted by quantum computers. If attackers were to record these calls, they could theoretically break the encryption once advanced quantum computers are developed. AWS's hybrid TLS seeks to address this scenario, and Echoworx anticipates implementing this in near future.

Adopt Post-Quantum Cryptographic Algorithms

Research Standards

Adhere to guidelines set by standardization bodies such as the National Institute of Standards and Technology (NIST)

NIST recently approved three post-quantum cryptographic algorithms:

FIPS 203 (ML-KEM)
FIPS 204 (ML-DSA) and,
FIPS 205 (SLH-DSA).

Echoworx plans to follow NIST recommendations by adopting hybrid encryption solutions, combining classical cryptographic methods with quantum-safe alternatives.

This approach aims to ensure a smooth transition from current encryption standards to post-quantum cryptography.

Upgrade Infrastructure

Hardware and Software Compatibility

Ensuring hardware and software compatibility is key.

Systems must support post-quantum cryptography (PQC) algorithms, which often demand greater computational power than traditional methods.

Transitioning to PQC will require overhauls to cryptographic libraries, protocols, hardware, and organizational practices. Echoworx plans a phased rollout, prioritizing compatibility, performance, and security at every step.

Build Organizational Awareness

Training and Education

IT teams and leadership must grasp the quantum threat and the role of post-quantum cryptography (PQC).

At Echoworx, all staff members receive ongoing training on evolving security threats and transformations, with a focus on email security and encryption. As PQC technology advances, Echoworx personnel will stay updated.

The Product Management team is leading the development of a roadmap toward a fully PQC-resistant product for global enterprises while ensuring knowledge sharing across the organization as the PQC landscape evolves.

Track Quantum Technology Advancements

Monitor Developments

Keep up with breakthroughs in quantum computing, cryptography, and evolving industry standards.

Echoworx has closely followed developments from NIST in recent years, alongside insights from industry experts and cryptographic leaders—and will continue to monitor these critical areas.

Conduct Regular Audits and Updates

Stay Ahead

Update cryptographic systems regularly as post-quantum cryptography (PQC) standards evolve.

Echoworx plans to integrate PQC algorithms into its infrastructure and applications, followed by annual audits and assessments to uphold its reputation for strong security.

Updates will be made promptly, aligning with best practices and long-term PQC planning.

ECHOWORX™

IT PAYS TO BE SECURE

Echoworx is leading the way in secure email encryption for the enterprise market. As quantum computing evolves, we remain ahead of the curve by proactively addressing the quantum threat. Through the adoption of post-quantum cryptography algorithms, infrastructure upgrades, and close monitoring of advancements in quantum technology, we are ensuring our solutions remain resilient.

In an enterprise landscape that demands foresight, Echoworx is not just reacting—we are setting the standard.