Chart Your Course to a Quantum-Safe Future

The quantum computing era is approaching—perhaps as soon as 2030. While it promises breakthroughs, it also threatens to break the encryption that currently protects our digital world. The journey to quantum safety has already begun. Is your organization prepared, or are you navigating without a map?

Your Starting Point: Are You Crypto-Blind?

Do you know what's securing your data's journey?

Many organizations can't answer a simple question: What cryptographic algorithms are protecting your data right now? This lack of visibility is the first major roadblock on the path to quantum safety.

You Can't Manage What You Can't See

Your environment is a complex mix of traffic secured by hundreds of different algorithms:

- Strong, modern algorithms
- Weak, outdated algorithms vulnerable even today
- Soon-to-be-obsolete algorithms that a quantum computer will break

Without visibility, you can't achieve crypto-agility. How can you steer your organization to safety if you don't know where you are starting from?

Dangers Ahead: The Quantum Threat Is Here Now

The quantum threat isn't a future problem—it has created new dangers today.

Quantum computers will render today's public-key encryption useless. Adversaries are exploiting this future inevitability now.

The "Harvest Now, Decrypt Later" Heist

THE THREAT

Malicious actors are capturing and storing your encrypted data today. They are creating massive archives of sensitive information, betting they can unlock it all once quantum computers are available.

THE IMPACT

Your most valuable long-term assets—intellectual property, source code, financial records, and state secrets—could be stolen and later exposed. Their journey was intercepted.

The Quantum Impersonator

THE THREAT

A quantum computer will be able to forge the digital signatures used in website certificates. This completely breaks the trust model of the internet.

THE IMPACT

Your users could be sent to a malicious website that looks and feels exactly like your trusted banking portal or Office 365 login. Every password, transaction, and data entered will be stolen in real-time.

Your Guide to a Seamless Transition to Quantum-Safety

Navigate the transition with confidence.
Zscaler is your partner for the quantum journey.

A successful transition doesn't require a "rip and replace" of your entire infrastructure. With the right cloud-native architecture, you can achieve quantum safety seamlessly.

Step 1: Discover and Map Your Terrain

ACTION

Gain 100% visibility into all cryptographic protocols and algorithms used across your environment.

HOW ZSCALER HELPS

We see and inspect all traffic, allowing you to identify weak algorithms and understand your crypto-posture. The fog is lifted.

Step 2: Build a "Quantum Bridge"

ACTION

Protect your data from "Harvest Now, Decrypt Later" attacks today, even if your servers and endpoints do not support post-quantum cryptography (PQC).

HOW ZSCALER HELPS

The Zero Trust Exchange acts as a bridge to quantum-readiness: It can secure the connection from Zscaler to a destination using a hybrid approach using classical-to-quantum (or vice versa) key exchange, making data with a long shelf-life quantum-resistant.

Step 3: Enforce and Stay Agile for the Road Ahead

ACTION

Set policies to require PQC for sensitive destinations and adapt as new cryptographic standards emerge.

HOW ZSCALER HELPS

Centrally manage your crypto policies from the cloud. As standards evolve, Zscaler updates its global security platform, the Zero Trust Exchange, ensuring your organization is always using the most current, secure algorithms without costly hardware upgrades or policy configuration changes.

Arrive Safely at Your Quantum-Safe Destination

Don't wait for the quantum storm to hit.
The journey to safety starts with visibility and a partner who can bridge the gap.
Begin your journey today.

LEARN MORE

Act Fast.
Stay Secure.