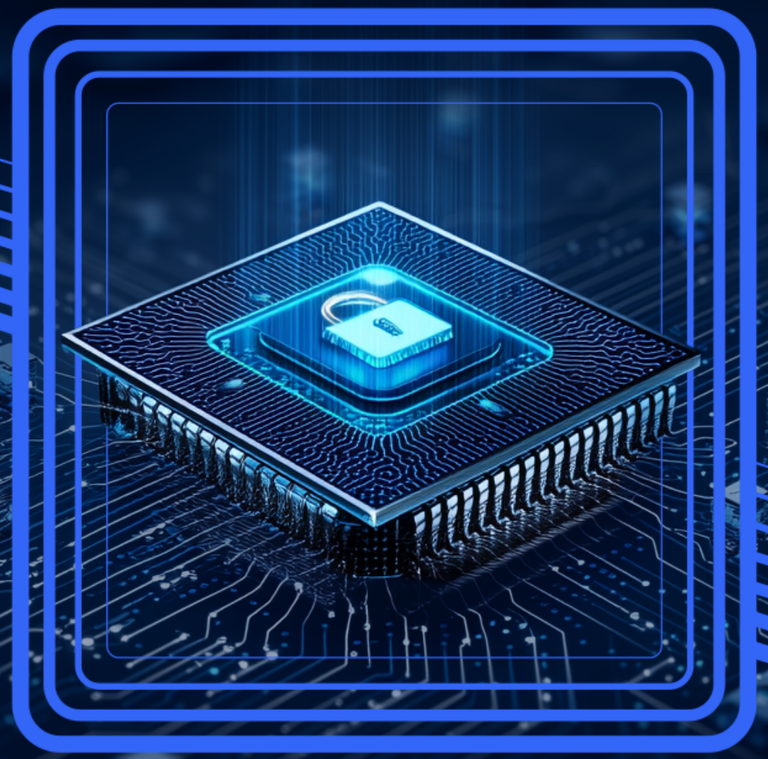
WHITEPAPER



The Quantum Tipping Point

Executive Guidance for Post-Quantum Readiness Without a Disruptive Overhaul

By Yaroslav Rosomakho, Chief Scientist at Zscaler & member of the Internet Architecture Board (IAB)

START

zscaler

THE RESILIENCE FACTOR

Introduction

In enterprise planning, horizon risks are well understood. They are known threats that remain distant, giving organizations time to prepare before impact. But this comfortable pace doesn't apply to quantum-based security threats, and the window for preparation is closing well before the tangible threat will materialize.

Quantum computing presents a future challenge to modern encryption systems — but it's one that requires action now. While current quantum systems cannot break modern public key cryptography at scale, **the breach of the Cryptographically Relevant Quantum Computer (CRQC) threshold — sometimes referred to as 'Q-Day' — could arrive as soon as 2030.** The date is uncertain; the lead time required to act on it is not.

Preparatory attacks are already happening, particularly by nation-state actors with access to vast volumes of data carried over networks. These adversaries are collecting encrypted data today, expecting to decrypt it later when sufficiently powerful quantum capabilities exist.

Will enterprises have transitioned to a state of post-quantum readiness (PQR) before the threat hits? Without early groundwork, they will remain exposed.

POST-QUANTUM READINESS (PQR):

Post-quantum readiness is the ability to identify where the cryptography your organization relies on is vulnerable to future quantum attacks, and to transition those components to quantum-resistant alternatives in a controlled and sequenced way. Understanding your current situation and planning for the transition are significant business challenges.

In this sense, quantum computing is perhaps better understood as a '**decision-horizon threat**'; one where the window to act decisively is shrinking, creating new risk in advance of the threat itself. 2026 is therefore a pivotal year if businesses are to strategically address the threat. **Indeed, we believe it must be considered as the quantum tipping point.**

Understanding All Three Quantum Risks

The ‘harvest now, decrypt later’ (HNDL) attack model that impacts data confidentiality is a well-publicized example of a threat that is both immediate and distant. Data from Zscaler’s recent research report, **The Ripple Effect: A Hallmark of Resilient Cybersecurity**, illustrates this point. Based on a survey of 1,750 IT leaders across 14 global markets, our report found that six in 10 business leaders believe data stolen today could pose a material risk to their futures, once that data becomes actionable with the advent of a CRQC.

But HNDL is only one challenge. The bigger business risk is trust. The digital signatures that underpin authentication, authorization and attestation across modern systems were not designed to withstand a future CRQC. When signatures fail, trust fails in real time — not years later. The required migration to post-quantum digital signatures will be highly complex and involve multiple timelines. Planning for it should be happening now.

Finally, the regulatory landscape is evolving. New compliance and regulatory requirements may arrive before the threat itself, with businesses at risk of reputational, financial, and legal damage if they lag on adoption. Further muddying the waters — and compounding the urgency — is the reality that no adversary will reveal if or when they have acquired cryptographically relevant quantum-computing capabilities. For an extended period, businesses will be hampered by that uncertainty when quantifying organizational risk and setting strategic prioritization. **To a significant extent, they will be flying blind.**

The quantum threat isn’t urgent simply because it is fast approaching. It’s urgent because the window for proactive mitigation is closing fast.

The operational reality is that awareness is rising faster than readiness — largely because most organizations still can’t quantify cryptographic exposure across protocols, environments, and vendors. The Ripple Effect report reveals that 52% of businesses agree their security systems can’t defend against current advanced threats, let alone emerging ones, making it harder to prioritize long-term work without a clear plan.

INSIGHTS SHARED

“In this paper, my aim is to translate these quantum threats into an executive plan for PQR. This will help leaders better understand all risks, quantify exposure, reduce the blast radius during migration, and build the agility to adapt as standards evolve.

Remember, PQR isn’t about predicting the exact arrival of Q-Day. It’s about protecting critical levels of confidentiality, trust and overall security, while preserving freedom of action, so you can migrate in a controlled, phased way before your options narrow.

To prioritize this prepared migration effectively, leaders need to focus on three core risk domains:

CONFIDENTIALITY: the potential capture and future decryption of data in transit today

TRUST: the future breach of current authentication systems

COMPLIANCE: the risk of falling into non-compliance with upcoming regulatory requirements”

YAROSLAV ROSOMAKHO
Chief Scientist at Zscaler & member of the Internet Architecture Board (IAB)

Why Now: The Decision–Horizon Risk

In a world defined by macroeconomic and geopolitical volatility, the immediate challenges facing businesses are numerous and difficult to prioritize.

It is understandable that a technological threat which has not yet materialized might be considered comparatively non–urgent. After all, current cryptography is broadly effective against tools that are available to adversaries today. Many security teams are also preoccupied and overstretched responding to AI–driven vulnerability discovery that demands rapid, often reactive defensive measures. Moreover, some businesses might consider themselves unlikely targets, perhaps because of their size.

But the threat posed by a future CRQC is **not one that can be mitigated by flipping a switch when the time comes**. The change required to reduce future exposure within a business is far–reaching. The risk is already here.

Post–quantum migration will be long, complex, and dependent on everything around you.

Long planning cycles are inevitable, comprehensive inventory of both hardware and software will be essential, and legacy and post–quantum cryptography (PQC) environments will be required to run in parallel during lengthy migration phases. Progress will be contingent on vendors, standards, partners, and replacement cycles.

Waiting for proof that a CRQC exists is not an option. Indeed, an extended period of uncertainty concerning the existence of such a machine is inevitable, because **adversaries will not advertise the capability.** The good news is that businesses still have lead time, if they act now.

KEY TAKEAWAY:

Misunderstanding the decision–horizon risk, and postponing action, will increase vulnerability and limit your ability to deliver a controlled and timely migration to post–quantum cryptography.

From Here to There: Current Cryptography and Post-Quantum Readiness

Cryptography is the unseen infrastructure of digital trust. Understanding where that infrastructure is, or could become, vulnerable is the foundation of any credible response to the quantum threat.

Modern digital systems rely on cryptography for three critical functions: to **secure the confidential exchange of data**, to **authenticate identities**, and to **maintain data integrity** across open networks.

Fortunately, not all modern cryptography is vulnerable to quantum threat. Modern symmetric cryptography and widely used cryptographic hash functions are expected to remain robust. The primary migration priority is **public-key cryptography** — specifically key exchange and digital signatures, which need to be replaced.

KEY EXCHANGE

This is the mechanism by which two parties establish a shared 'secret' over an untrusted medium such as the Internet. This shared secret is then used to derive other keys using a protocol-specific key schedule. Modern protocols such as TLS, SSH, IPSec, and WireGuard rely on key exchange algorithms such as ECDHE that are based on mathematical problems that a CRQC could crack. Key exchange vulnerability is the primary risk associated with HNDL attacks.

DIGITAL SIGNATURES

This is the mechanism by which the identity and integrity of users, devices, servers, websites, and workloads are verified. Current widely deployed signature schemes — including RSA, ECDSA, and EdDSA — underpin the trust and authentication frameworks that organizations rely on across virtually every digital interaction. They are embedded not just in website certificates but in user credentials, signed tokens, hardware security devices, and the public key infrastructure (PKI) that operates at scale across modern enterprises. The quantum threat to digital signatures is that, with the (potentially unknown) advent of a CRQC, all authentication and trust is negated.

KEY TAKEAWAY:

PQR is a sequencing challenge, not a blanket replacement exercise. The immediate priority is to focus on key exchange, closely followed by digital signatures.

Three Key Risks: Underpinning the Need for Migration

Quantum computing creates three primary security risks for businesses. Understanding these helps illustrate why migration is a matter of urgency.

1. **Confidentiality:** HNDL attacks exploit the vulnerability of current key exchange mechanisms. Data intercepted at any point before migration to post-quantum key exchange has been completed remains at risk of future decryption once a CRQC exists. Every day that migration is delayed adds to the pool of data available to adversaries for future exploitation.

2. **Trust:** Digital signatures do not create the same HNDL exposure as encrypted traffic, but they create a different trust-continuity problem. A CRQC could allow adversaries to forge signatures or undermine confidence in existing trust chains, including certificates, software updates, firmware, signed tokens, and long-lived records. This would eliminate the ability to securely authenticate, authorize and attest users, devices, servers, and workloads.

3. **Compliance:** Governments and regulatory bodies are already setting explicit timelines for post-quantum cryptography, to retire or disallow quantum-vulnerable cryptography by 2030—2035. This is evident in the IR 8547 roadmap released by NIST (outlining how and when organizations should transition to quantum-safe cryptography) and the recent U.S. executive order EO 14412 mandating that government systems migrate to quantum-safe cryptography. Even if a CRQC wasn't available until 2050, businesses would likely be at risk of non-compliance years earlier.

Added to these risks is the likelihood that the 'confirmed' existence of a CRQC might not be known. As such, **migration to post-quantum cryptography is a near-term strategic imperative.** That said, each of these three risk areas has unique drivers, requirements, and urgency profiles, as set out in the table on the following page. Leaders can use this insight to lay the groundwork for migration.

Risk Profiles: How They Impact Migration Plans

	Confidentiality	Trust	Compliance
Migration driver	Prevent future decryption of data in transit today	Preserve the ability to authenticate users, devices, and systems	Maintain compliance ahead of externally imposed deadlines
Threat timeframe / trigger	Data that's being harvested today	Triggered when a CRQC exists	Regulatory deadlines. Independent of technical timeline
Urgency level	Immediately urgent considering data is already being harvested today	Urgent due to complexity and lead time. Not due to an active attack today	Regulator-dependent
Migration scope	Bounded: defined set of key exchange protocols	Broad: embedded across certificates, credentials, hardware, and PKI hierarchies	Applies across all vulnerable cryptography
Migration approach	Incremental: libraries and configurations can be upgraded progressively	PKI trust chain must be post-quantum from end to end before protection is achieved	Dictated by regulatory guidance and deadlines
Hardware challenge	Low: primarily software and configuration challenge	High: security keys, TPMs, HSMs, and secure enclaves require replacement	Variable
Parallel running required?	Hybrid and fallback modes may be needed during transition	Yes. Classical and post-quantum PKI may need to operate simultaneously during transition	Dependent on regulatory requirements
Migration complexity	Moderate	High	Variable

KEY TAKEAWAY:

Confidentiality, trust, and compliance each create different pressures, but they converge on the same conclusion: post-quantum migration is not optional. The only real choice is whether that migration happens in a phased, controlled way or under growing constraint.

The PQR Playbook: See, Contain, Sustain

For all the depth of the quantum threat, its knowns and unknowns, businesses have a **clear opportunity** to prepare and protect themselves. By taking decisive action today, business leaders can mitigate the risks they will face tomorrow.

Delivering post-quantum readiness will require a combination of specialist skills that many organizations don't yet have. While elements of this work (such as asset inventory, risk prioritization, and program governance) can often be led in-house, more complex activities including cryptographic discovery, protocol remediation, and architecture redesign may require external expertise. In practice, most organizations will adopt a hybrid model: retaining strategic control internally while drawing on specialist partners to accelerate execution in high-complexity areas. The key is to build internal understanding and ownership early, so that PQR becomes a sustained capability rather than a one-off transformation.

What follows is an action plan to guide your business's migration. Built for decision-makers, this plan helps enterprises **minimize the disruption, exposure, and loss** of trust inherent in the quantum threat they face.

Crucially, the approach must be carefully sequenced.

EVOLVING TO POST-QUANTUM READINESS: STRATEGIC APPROACH

SEE IT
Identify and quantify your exposure to the emerging quantum threat so you can prioritize effectively

CONTAIN IT
Introduce guardrails to reduce your exposure during the phased transition to PQR

SUSTAIN IT
Build the capacity to respond rapidly to changes in standards and technological advances

The PQR Playbook: How To Sequence

Sequencing the migration process **provides a structure that eliminates the risks** of both rushed early action and late, panicked action. It breaks enterprise approaches into **achievable steps** that can be more easily managed in the correct order, even against the backdrop of existing geopolitical, macroeconomic, and other technological challenges.

By initiating this process today, leaders will avoid having to tackle a potentially insurmountable challenge in a few years' time.

INSIGHT: THE AWARENESS-TO-ACTION GAP

Our Ripple Effect research shows that many businesses already recognize quantum as a credible future threat, yet that recognition is still failing to translate into concrete planning because cryptographic exposure remains difficult to see clearly.

That visibility gap is what turns awareness into inertia. If leaders cannot gauge which systems, protocols, and trust chains are most exposed, they cannot make a credible case for investment or build a phased migration plan. The research reflects exactly that disconnect: **55% of businesses struggle to quantify their exposure** to the quantum risk, despite believing the risk to be significant, and **57% have not yet factored post-quantum cryptography** into their cybersecurity strategy.

SEE IT:
Quantify Your Exposure.

You cannot prioritize what you cannot see, so visibility must become the foundation of your response. To do this, you must build a comprehensive inventory of assets and exposure that allows you to both understand required action and communicate the need for prioritized investment. Do not rely on guesswork and assumption.

Understand your risk across both key exchange and digital signature environments. Key exchange inventory is bound to a defined set of specific protocols, including TLS, SSH, IPSec, and WireGuard. Digital-signature inventory is a tougher challenge. It spans certificates, user and workload credentials, and hardware dependencies.

Platforms that can surface which cryptographic algorithms are actually in use — based on live traffic rather than static inventories — will help your team turn **'awareness' into measurable exposure.** Zscaler offers this kind of post-quantum cryptography visibility to support this shift.

The Visibility Shift:
From risk awareness to measurable exposure.

CONTAIN IT:

Reduce the Blast Radius During Migration.

Migration to quantum-resistant systems, while a universal imperative, **cannot be simultaneous** across all exposed systems. Businesses must be prepared for extended periods of combined operation, running both legacy and PQC systems.

A critical first step in this phase is to identify the legacy systems and appliances that will be most difficult and time-consuming to upgrade, and build safeguards around the data they process.

Here, you have two options:

- **Reduce data sensitivity**
  Ensure nothing that could constitute a business risk is carried over legacy channels. Data at risk of being harvested today should be irrelevant by Q-Day.
- **Encapsulate legacy traffic within a PQC tunnel**
  Establish a fresh PQC connection to the destination, regardless of the originating system's capabilities, and effectively extend post-quantum protection to systems that cannot yet be upgraded.

During this migration phase — when some systems can't be upgraded quickly — organizations benefit from a **broker layer** that can encapsulate legacy traffic and establish fresh connections onward, reducing exposure even when endpoints aren't yet post-quantum capable. **Zscaler's Zero Trust Exchange** provides a practical way to do it.

The Containment Shift:
From hoping legacy holds to designing for safe transition.

SUSTAIN IT:
Build Resilience Through Crypto Agility

Quantum computing will bring a new level of instability to what has previously been the relatively stable world of cryptography. Resilience will no longer be defined by the strength of a current system, but by remaining **sufficiently adaptable** to respond rapidly in an environment of constant change.

The reality is that post-quantum cryptography itself may become vulnerable as quantum and AI enabled cryptanalysis evolves. **The ability to change cryptographic primitives** — key exchange algorithms, symmetric ciphers, hashes, and digital signature schemes — quickly and deliberately, and without the upheaval associated with an unplanned pivot, will become essential. In this model, these primitives are not hard-coded into systems and infrastructure. They can be swapped at relatively short notice as circumstances require.

The transition to post-quantum cryptography is unlikely to be a one-time upgrade after which things settle down. Other disruptive developments, unforeseen today, may demand further rapid transitions in future. **This shift toward adaptable cryptographic infrastructure** allows organizations to respond to that uncertainty without crisis. The goal is to make cryptographic change a repeatable operational capability rather than an exceptional and disruptive event.

Crypto agility becomes real when organizations can centrally set — and update — which cryptographic primitives are negotiated and do so surgically by context. **Zscaler is developing crypto profiles** to give customers that kind of control as standards and threats evolve, including:

- The ability to enforce PQC rather than just attempt it as best-effort
- The ability to enforce stronger (more compute-intensive) algorithms for highly sensitive data
- Surgical control over cryptographic preference per client and server
- Compliance to various regulatory requirements that may be conflicting across verticals and geographies

The Sustain Shift:
From one-time upgrade to long-term resilience capability.

The PQR Playbook: Summary

	Challenge	Learning	Action
Visibility	Exposure is not well understood	Visibility is essential to prioritization and investment	Build a comprehensive inventory of systems in use
Containment	Different legacy systems have different migration profiles	Migration will be uneven and involve parallel legacy and PQC operation	Implement guardrails to reduce exposure during transition
Sustainment	Post-quantum algorithms are new and may themselves require further migration	Agility is the new operational imperative	Make cryptographic change a repeatable operational capability

KEY TAKEAWAY:

PQR depends on doing the right work in the right order: first make exposure visible, then reduce the blast radius during transition, then build the agility to keep adapting as standards and threats evolve.

Quantum Resilience: The Tipping Point for Readiness

The quantum threat might not announce itself. And while Q-Day may still be years away, simply waiting for proof of the threat will leave no time for a controlled transition. Businesses that achieve post-quantum readiness will be those that recognize early that the decision horizon is the real deadline.

The path is clear.

SEE IT: build the visibility and inventory that makes prioritization possible.

CONTAIN IT: implement the guardrails that reduce exposure while migration proceeds.

SUSTAIN IT: make cryptographic agility a permanent operational capability, not a one-time project.

Resilience is not built in response to disruption; it is built before disruption arrives. The tipping point is here and the time to act is now.

ARE YOU READY?

THE PQR LITMUS TEST: As a leader, you should ask yourself the following questions. If you answer 'no' to any of them, your organization is vulnerable to quantum threats; today and in the future.

Three questions every leader should ask:

1. Do we know how and where our sensitive data may be exposed?
2. Do we have a live and current inventory of all cryptographic systems and protocols?
3. Do we have guardrails for cryptographic systems and protocols?

GET STARTED

The shift to post-quantum cryptography doesn't have to be all-or-nothing. Zscaler's Zero Trust Exchange helps organizations expose, reduce, and manage cryptographic risk in real time — from discovery through to long-term control.

LEARN MORE ABOUT ZSCALER'S ZERO TRUST EXCHANGE

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com

Zscaler, Inc. (Worldwide HQ), 120 Holger Way, San Jose, CA 95134, United States

zscaler.com