From visibility to action

Why post-quantum readiness will fail without cryptographic visibility

June 2026

The better the question.
The better the answer.
The better the world works.

EY

Shape the future with confidence

Contents

From visibility to action

Why post-quantum readiness will fail without cryptographic visibility

Executive summary

Post-quantum cryptography (PQC) is rapidly moving from a future consideration to a present-day enterprise risk. While much attention has focused on quantum-safe algorithms and standards timelines, many organizations are overlooking a more fundamental barrier to readiness: the lack of visibility into their existing cryptographic environments. Cryptography is deeply embedded across networks, applications, identities, devices and third-party services, often without centralized ownership or governance.

At the same time, two notable shifts are increasing the urgency to act. First, certificate lifetimes are shrinking, driving higher operational complexity and increasing reliance on automation and continuous monitoring. Second, regulatory and standard-setting bodies across major jurisdictions are issuing increasingly concrete guidance on post-quantum transition planning, signaling heightened scrutiny of cryptographic controls and preparedness. As certificate lifetimes shorten, encrypted traffic grows and regulatory expectations intensify; this cryptographic opacity turns PQC migration into a high-risk endeavor.

This white paper posits that cryptographic visibility is the foundation of post-quantum readiness. By combining enterprise-level strategic leadership with platform-enabled, real-time visibility into encrypted environments, organizations can align with emerging regulatory expectations and move from awareness to actionable, defensible progress.

Quantum risk has become an execution problem

Quantum computing risk is no longer a distant, theoretical concern. Across regions, regulators and standards, bodies are signaling that organizations must begin preparing now for a post-quantum transition — not because quantum computers are fully realized today, but because cryptographic change takes years to plan and execute.

For most enterprises, the limiting factor is not algorithm availability. It is execution readiness: the ability to identify cryptographic dependencies, prioritize remediation and change controls without disrupting critical business processes. As regulatory expectations accelerate, this execution gap becomes a material business and compliance risk.

Quantum computing risk is no longer a distant, theoretical concern.

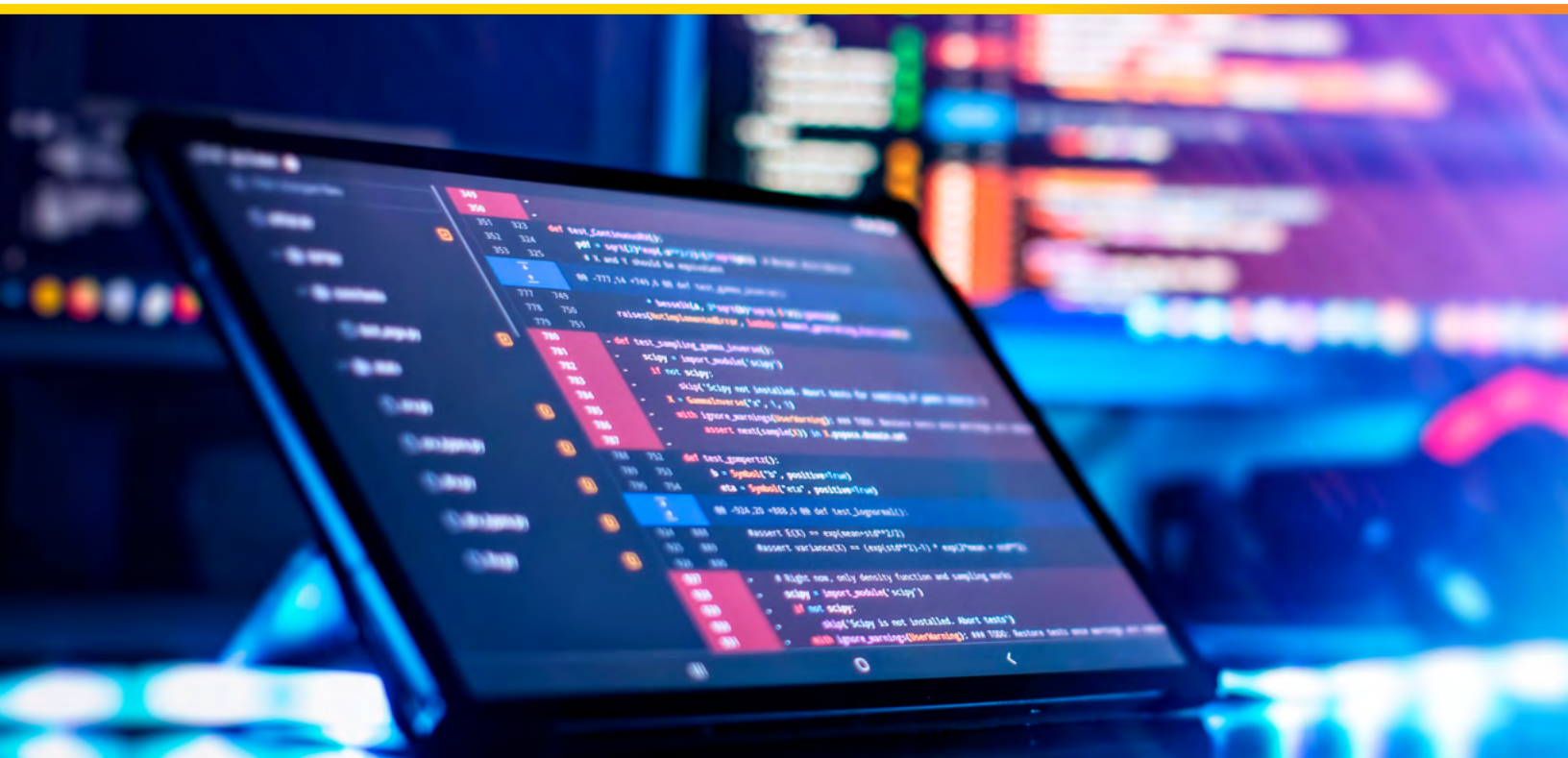
Cryptographic blind spots are the real blocker

Across jurisdictions, PQC guidance consistently emphasizes early discovery, inventory and prioritization. Regulators expect organizations to understand their cryptographic estates to form a long-term strategy for transition, while addressing the governance and regulatory frameworks.

Cryptographic visibility enables organizations to:

- Inventory cryptographic assets across networks, applications, identities and data flows
- Identify quantum-vulnerable dependencies, including hard-coded libraries and legacy protocols
- Prioritize remediation based on regulatory exposure, business criticality and data longevity
- Support crypto-agility, enabling phased, auditable transitions aligned with evolving standards
- Demonstrate progress as reporting and oversight requirements increase

As certificate lifetimes shorten and encrypted traffic dominates enterprise environments, continuous visibility becomes essential — not only for security but also for regulatory confidence. Without it, compliance timelines may be set externally, but execution risk remains internal.



Why shrinking certificate timelines and regulation raise the stakes

Two structural shifts are accelerating the urgency to address cryptographic visibility.

1. **Certificate lifetimes are collapsing.**

   The move toward significantly shorter Transport Layer Security (TLS) certificate lifetimes dramatically increases the frequency and operational impact of cryptographic change. Environments that were manageable with long-lived certificates quickly become fragile without accurate inventories, automation and continuous monitoring.

2. **Regulatory expectations are hardening.**

   Across major jurisdictions, regulators and standard-setting bodies — including the National Institute of Standards and Technology (NIST) in the United States, the European Telecommunications Standards Institute (ETSI) and the European Commission, Germany's Federal Office for Information Security (BSI), Australia's Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC), and the Canadian Centre for Cyber Security — are issuing increasingly concrete guidance and roadmaps for transitioning away from quantum-vulnerable cryptography. Fast-approaching timelines reduce tolerance for ad hoc or reactive approaches to cryptographic change.

Visibility is the foundation of post-quantum readiness

Cryptographic visibility enables organizations to move from abstract concern to informed decision-making. At its core, visibility means not only understanding what cryptography exists, but also where it is used, how it is managed, and which business processes depend on it.

Effective visibility allows organizations to:

- Identify high-risk systems and long-lived data early
- Sequence remediation based on impact rather than intuition
- Reduce operational disruption through phased migration
- Support crypto-agile architectures as standards evolve

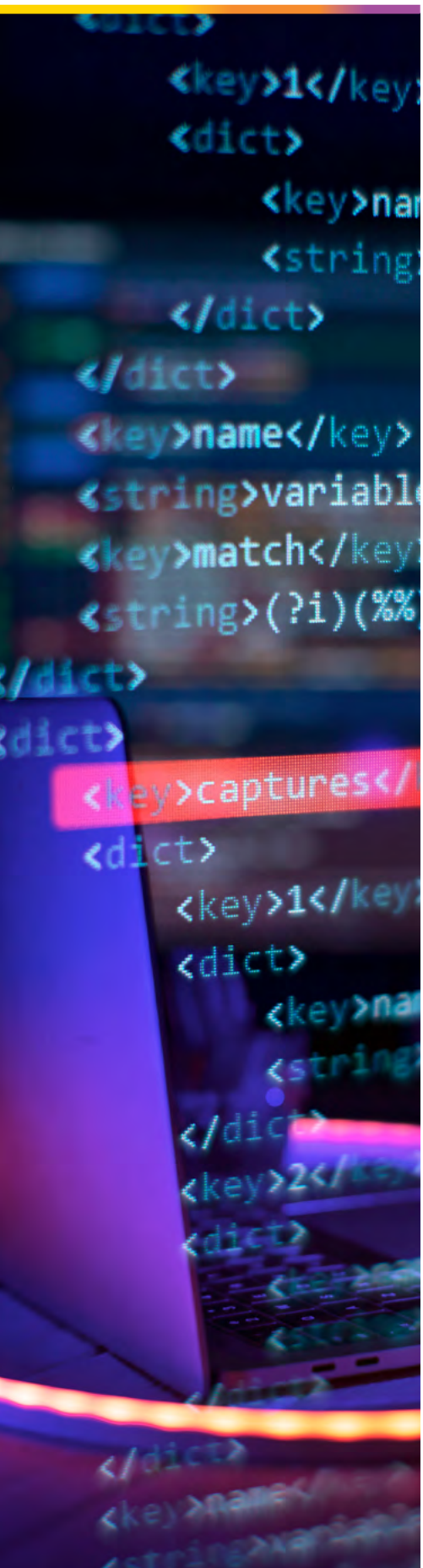
Without this foundation, even well-intentioned PQC initiatives struggle to move beyond pilots and proofs of concept.

Platforms enable scale — leadership enables success

Large-scale cryptographic visibility is difficult to achieve through manual processes alone, particularly in environments dominated by encrypted traffic, cloud services and distributed users. As a result, many organizations are evaluating security and networking platforms that operate in line with enterprise traffic flows and can provide telemetry on cryptographic protocols, certificates and encryption usage at scale. Capabilities often considered include:

- Visibility into encrypted traffic patterns and protocol usage
- Discovery of weak, deprecated or quantum-vulnerable cryptographic configurations
- Inventory of certificates, keys and cryptographic dependencies across environments
- Support for continuous monitoring, automation and auditability

These capabilities, when combined with strong governance and risk alignment, can help organizations move from exploratory assessments to defensible execution.



From strategy to execution: aligning leadership, governance and technology

Meeting accelerating PQC timelines requires both strategic direction and operational capabilities, such as technology and tooling upgrades. PQC readiness is a transformation challenge that spans strategy, governance, risk and operations.

Organizations must:

- Frame PQC as an **enterprise risk and resilience issue**, not a narrow cryptographic upgrade
- Establish clear ownership and accountability for cryptographic decisions
- Translate regulatory guidance into **sequenced, auditable execution plans**
- Enable continuous insight into how cryptography is deployed, managed and changed over time

Technology platforms can play an important enabling role by supporting discovery, monitoring and control at scale. Real-time insights into encrypted data and traffic allow organizations to gather critical data and manage potential "store now, decrypt later" threats.

With platforms as data aggregators, leadership can contextualize technical findings within business priorities, regulatory exposure and long-term architectural direction. These inputs are critical for long-term security strategies tailored for risk profiles and help organizations remain resilient against emerging threats.

Successful organizations treat cryptographic visibility as a capability toward crypto-agility — integrating it into ongoing security operations, risk governance and change management processes.

Board-level challenges to address:

- **Legacy crypto limits agility.**

  Critical systems often rely on embedded or hard-to-change cryptography, requiring phased and hybrid transition strategies rather than immediate replacement.

- **Visibility gaps create hidden risk.**

  Blind spots across unmanaged assets, applications and third-party services delay migration and complicate regulatory reporting.

- **Operational complexity is rising fast.**

  Shorter certificate lifetimes and growing encrypted traffic volumes demand automation and continuous monitoring, without sacrificing governance or auditability.

Encrypted traffic visibility as a core quantum-safe capability

Encrypted traffic is now the dominant attack surface. Adversaries routinely exploit encryption to conceal malware, phishing, crypto mining and data exfiltration. Zscaler's State of Encrypted Attacks Report notes that encrypted threats accounted for 87% of all attacks detected and blocked. As PQC is adopted, encrypted traffic — quantum safe or otherwise — will remain a primary vehicle for attackers. In addition, as quantum-safe algorithms are introduced, encrypted traffic — whether classical or post-quantum — will remain a critical area of regulatory focus.

Effective cryptographic oversight increasingly depends on enterprise-scale platforms that operate in line with global traffic flows, spanning cloud, network and user environments. At scale, such platforms process vast volumes of encrypted communications in real time, enabling consistent policy enforcement, continuous monitoring and centralized insight across geographies and operating environments.

From a regulatory and execution standpoint, an enterprise-grade security platform should enable organizations to:

- Inspect and control post-quantum encrypted traffic
- Protect against future risks, such as "store now, decrypt later" attacks
- Preserve an accurate inventory of certificates, keys and cryptographic controls
- Maintain cryptographic inventory and visibility
- Support regulatory audits and reporting without disrupting operations

When combined with scaled governance, ownership and risk alignment, these capabilities allow organizations to manage cryptographic change as a **continuous, defensible control** rather than a one-time remediation exercise. This approach supports quantum safety and helps meet regulatory compliance.

What leaders should do now

Organizations must take proactive steps to enhance visibility into their cryptographic environments to address quantum risk and meet evolving regulatory expectations. This begins with understanding where cryptography exists today, and how it supports critical business processes.

By pairing strategic leadership with platform-enabled visibility, organizations can reduce execution risk, prioritize effectively and build a credible, defensible path to post-quantum readiness.

Conclusion

Post-quantum cryptography is not a future upgrade — it is a present-day execution challenge. Organizations that focus only on algorithms risk discovering too late that they cannot deliver within shrinking timelines.

Those that begin with visibility are better positioned to migrate safely, demonstrate progress and adapt as standards and regulations evolve. A proactive approach to cryptographic visibility strengthens not only quantum readiness but also overall cyber resilience in an increasingly encrypted world.

Authors

Joe Depa
Partner
Ernst & Young LLP
joe.depa@eyg.ey.com

Rodrigo Madanes
Director
Ernst & Young LLP
rodrigo.madanes@ey.com

Biren Agnihotri
Partner
Ernst & Young LLP
biren.agnihotri@ca.ey.com

Varun Sharma
Principal
Ernst & Young LLP
varun.sharma7@ey.com

Richard Watson
Partner
Ernst & Young
richard.watson@au.ey.com

Perris Kusilek
Senior Manager
Ernst & Young LLP
perris.kusilek@ey.com

Nary Dolan
Associate Director
Ernst & Young LLP
nary.dolan@ey.com

Kartheek Solipuram
Associate Director
Ernst & Young LLP
kartheek.solipuram@ey.com

Adam Berman
Global Alliances Director
Zscaler, Inc.
aberman@zscaler.com

Brendon Macaraeg
Senior Product Marketing Manager
Zscaler, Inc.
bmacaraeg@zscaler.com

Additional contributors

Naveed Mahmood
Manager
Ernst & Young LLP
naveed.mahmood@ey.com

Kristopher Kolk
Staff
Ernst & Young LLP
kristopher.kolk@ey.com

This white paper posits that cryptographic visibility is the foundation of post-quantum readiness. By combining enterprise-level strategic leadership with platform-enabled, real-time visibility into encrypted environments, organizations can align with emerging regulatory expectations and move from awareness to actionable, defensible progress.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

US SCORE no. 31256-261US
CSG no. 2603-10905-CS
ED None

ey.com