NAVIGATING THE QUANTUM SHIFT

A Practical Roadmap to Prepare for the Next Wave of Threats

paloalto NETWORKS | CIO DIVE

Custom content for Palo Alto Networks from Studio by Informa TechTarget

The cryptographic infrastructure that supports secure internet communications faces a foundational change. Current encryption methods have protected enterprise systems for five decades. Yet cryptography experts, industry analysts, and government agencies project that quantum computers will break these algorithms, possibly as early as 2030.

The risk is no longer hypothetical. And the window to achieve quantum-safe security is closing.

Enterprise-wide migration to quantum-safe security takes an estimated three to five years. The level of effort is significant and spans multiple business and technology domains.

For executive leaders, the challenge is threefold:

- **Organizational:** Unlike other transformational initiatives, modernizing the cryptographic infrastructure protects existing capabilities rather than fueling innovation. To secure board-level investment for this invisible threat, board conversations must focus on compliance exposure, regulatory deadlines, and the long-term value of the data that adversaries are already collecting.

- **Operational:** Executing this multi-year infrastructure project is complicated. You need to inventory cryptographic usage and dependencies across thousands of systems, coordinate migration across a fragmented vendor ecosystem, and maintain business continuity throughout the transition.

- **Technical:** Although post-quantum algorithms are mathematically proven, the libraries implementing them have not been battle-tested as extensively as current cryptography. You need to navigate evolving standards and implementations to understand which algorithms to implement and when.

With practical tools and a phased approach, quantum security becomes manageable rather than overwhelming. This playbook provides a strategic roadmap to help address all three challenges and begin the transition.

paloalto NETWORKS

The Quantum Threat: What's at Stake

Most digital systems use public key cryptography for data confidentiality, integrity, and authentication. To encrypt data in motion and at rest, current algorithms rely on mathematical problems that conventional computers would take billions of years to solve. Since quantum computers evaluate solutions simultaneously rather than sequentially, they can reduce the timeline to hours or days.

Industry experts expect that quantum computers capable of breaking current encryption will arrive as early as the end of this decade. The impact will be widespread, creating vulnerabilities for areas such as:

- **Secure communications:** VPNs, SSL/TLS protocols protecting web traffic, email, cloud connections
- **Identity and authentication:** Digital signatures and certificates, authentication systems, identity and access management platforms
- **Applications and infrastructure:** Web browsers, APIs, software distribution and signing, cloud services and databases
- **Embedded systems:** IoT devices, operational technology, outdated hardware

The business implications extend beyond data breaches and can include noncompliance risk, business disruption, and loss of customer trust. A simple way to think of the problem is: which data, when exposed in three to five years, will create serious problems for your organization and your customers?

Regulatory compliance: The US National Security Agency's CNSA 2.0 will begin enforcing post-quantum cryptography (PQC) for National Security Systems (NSS) in 2026, with key milestones for new NSS acquisitions by 2027 and full transition through 2035. The UK National Cyber Security Centre and the EU NIS2 Directive have established similar, non-optional timelines for critical sectors and "essential/important entities" PQC migration. As these mandates accelerate PQC adoption timelines across government and critical infrastructures supply chains, organizations risk penalties, financial liability, and the loss of government and essential services contracts.

Operational disruption: NIST has proposed deprecating quantum-vulnerable algorithms after 2030 and disallowing all quantum-vulnerable algorithms by 2035. A failure to proactively migrate to PQC and architect systems with "crypto-agility" (the ability to rapidly swap algorithms) may be viewed as a failure of due care by auditors and regulators. Expired or noncompliant certificates and protocols can trigger outages across identity systems, payments, APIs, IoT devices, VPNs, and integrations.

Erosion of digital trust: Weak security due to vulnerable encryption can cause customers, partners, and investors to lose confidence. This erosion of trust may create a competitive disadvantage.

The challenge is strategic rather than technical. Rather than waiting to react, forward-thinking organizations are taking advantage of new tools such as the Palo Alto Networks Quantum-safe Security to understand their cryptographic posture and plan systematic migration now.

Why You Need to **Accelerate Cryptographic Modernization**

Organizations cannot wait to act until cryptographically relevant quantum computers arrive. The most immediate threat is already underway.

Data storage has become inexpensive, and global connectivity is abundant. These elements make it viable for nation-state actors and well-resourced adversaries to harvest massive amounts of data today and decrypt once quantum computers become available.

The National Security Agency publicly warns that these invisible "harvest now, decrypt later" attacks are happening in the wild. Any data valuable beyond five to ten years is at risk today, including intellectual property, proprietary research, healthcare records, and sensitive personal data.

NIST Recommends Immediate PQC Implementation

When releasing the first post-quantum cryptography standards in August 2024, NIST urged organizations to "start integrating them into their systems immediately, because full integration will take time." The agency noted that historically, algorithm transitions have required 10-20 years to be implemented across information systems.

> "Regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing."
>
> - NIST

paloalto NETWORKS

Other factors are converging to create urgency for organizations:

Enterprise-wide migration typically takes three to five years. Organizations that don't start soon will be behind the curve as regulations gain momentum and AI advances the arms race, including cryptanalysis capabilities.

Technology leaders such as Google (which is adopting PQC for its Chrome browser) and AWS (which is rolling it out for key security services) will create ripple effects across their customers. That means your vendors and partners will start deprecating older algorithms.

Cyber insurance underwriters are incorporating quantum-aware risk modeling. Organizations that don't act proactively will likely see higher premiums. Surveys show that nearly half of cybersecurity professionals believe cryptographic risk will increase cyber insurance costs.

Waiting also expands your risk of rushed migration, including flawed implementation and missteps that compromise the transition.

Understanding the **Migration Realities**

Organizational, technical, and operational barriers can prevent successful execution. Avoid a rushed implementation by planning for these challenges early on.

Organizational inertia: PQC migration competes with other priority initiatives that have promising returns. Create a sense of urgency in the boardroom to gain support for the inventory and migration efforts.

Visibility gaps: Most organizations lack a comprehensive view of encryption practices across their infrastructure, from on-premises, data center, and branch locations, to applications, IoT systems, and user devices. A centralized discovery platform can automate cryptographic inventory and provide continuous visibility.

OT and IoT systems: Many medical devices, critical infrastructure systems, and manufacturing equipment cannot be upgraded without disruption, if at all. Cipher translation technology, available in Palo Alto Networks' PAN-OS software, allows instant device upgrades to quantum-safe status without downtime.

Complex migration process: Technology partners, vendors, and cloud providers are implementing PQC at varying timelines, which can create interoperability risks. Engage stakeholders early about their roadmaps, prioritizing relationships where migration support already exists, and building quantum readiness into your vendor evaluation.

Untested implementations: Unlike classical encryption, first-generation PQC code has not yet undergone decades of real-world hardening. NIST recommends a hybrid combination of classical and post-quantum algorithms to ensure systems remain secure if one of the components becomes vulnerable.

PQC algorithms are more resource-intensive, creating bottlenecks in older infrastructure.
PAN-OS 12.1 Orion enables quantum readiness on existing fourth- and fifth-generation firewalls, while the PA 5500 series of next-gen firewalls delivers up to four times the performance for high-volume environments that require dedicated hardware acceleration.

A Strategic Roadmap to **Quantum Security**

Cryptographic agility is central to the journey to quantum security. Agility enables upgrades and replacements of algorithms quickly and without disruption. As the Cyber Threat Alliance states, "Quantum risk is probabilistic, cascading, and difficult to reverse. In that context, cryptographic agility is not just a mitigation tactic—it's an operational obligation."

The roadmap below provides a framework for a multi-year, systematic transformation. These five phases often overlap rather than proceeding sequentially, and cryptographic agility serves as both a design principle and operational capability.

Phase 1:
Build organizational readiness
Core activities:

- Educate and align the C-suite on the urgency of quantum risk and make the business case for a multi-year investment.
- Secure funding and buy-in from the board and other executives.
- Identify personnel responsible for migration execution across different teams.

Phase 2:
Discover and assess
Core activities:

- Inventory all hardware and software assets to identify encryption protocols and categorize them.
- Assess whether hardware assets have sufficient compute to support PQC algorithms, and determine which will require upgrades or replacements.
- Identify vendors and partners across your infrastructure and discuss their PQC roadmaps, migration support capabilities, and ability to support algorithm substitution.
- Prioritize systems based on data sensitivity and lifespan, potential business impact if compromised, and susceptibility to attack.

Palo Alto Networks' Quantum Readiness Assessment

Strata Cloud Manager automates cryptographic inventory across devices, applications, and systems without requiring additional sensors. The platform categorizes assets as secure (post-quantum ready), weak (quantum-vulnerable), or vulnerable (deprecated ciphers), and provides upgrade recommendations.

paloalto NETWORKS

Phase 3:
Achieve quantum readiness
Core activities:

- Replace or upgrade hardware unable to support PQC, and upgrade software on compatible systems.
- Conduct proof-of-concept deployments in controlled environments using hybrid approaches that combine classical and post-quantum algorithms.

Quantum readiness is an operational and infrastructure state achieved when your environment can support post-quantum cryptography.

Phase 4:
Deploy to Quantum Secure
Core activities:

- Roll out PQC in phases, starting with the highest-priority systems.
- Ensure configurations enforce quantum-safe algorithms by default and automatically block deprecated algorithms when technically feasible.
- Update security policies to manage both classical and quantum-safe traffic during the transition period.
- Use proxy solutions such as cipher translation to make IoT devices quantum-ready when they cannot be updated directly.

Quantum secure is the operational state where PQC is actively deployed, configured, and enforced across sessions, user devices, and data.

Phase 5:
Maintain cryptographic agility
Core activities:

- Monitor for algorithm vulnerabilities and emerging threats, recognizing that post-quantum standards remain in early adoption and will mature over time.
- Establish rapid-response protocols to replace or update vulnerable algorithms.

Forging Partnerships for a **Path Forward**

Quantum readiness takes collaboration across the security industry, and solutions are maturing to help organizations prepare now. Those who begin their transition today position themselves to comply with regulations, protect against emerging threats, and maintain trust and business continuity.

Palo Alto Networks provides the platform, tools, and expertise to guide you through this shift, from initial assessment through deployment and ongoing cryptographic agility. Working with an expert partner can turn a daunting undertaking into an achievable, successful transformation.

Take the first step toward quantum resilience by exploring this CISO's Guide to Quantum Security, crafted by Palo Alto Networks experts.

paloalto NETWORKS

Studio
by informa techtarget

Expert led.
Impact driven.

Studio is Informa TechTarget's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Learn more