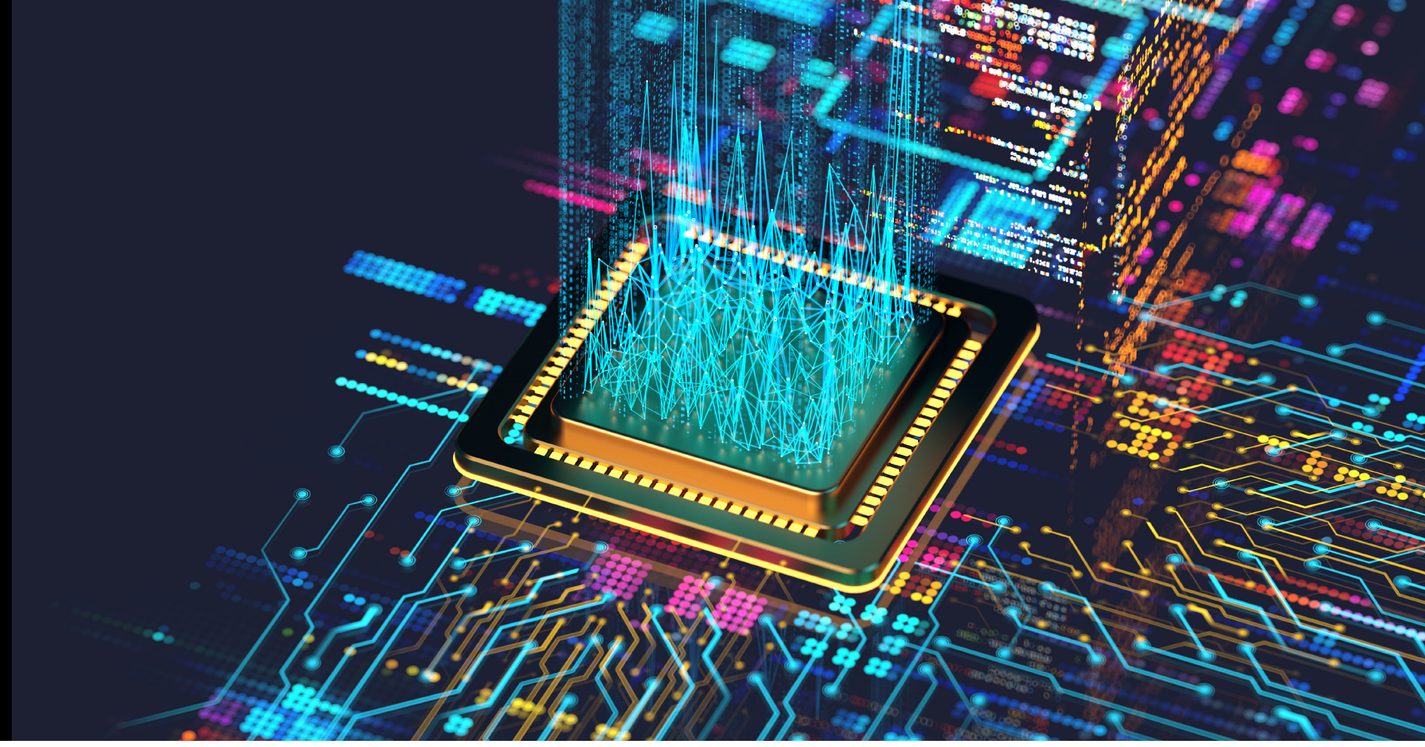
Industry Pulse

Quantum-Ready Security:
The Time to Act is Now

Powered by **DIVE**MARKETPLACE



Key Discussions

01

Cyber Resilience in the Post-Quantum Era: The Time of Crypto-Agility

TechRadar

02

The Clock is Ticking on AI Security in a Quantum World

Forbes

03

Preparing for a Quantum-Safe Future Should Begin Today

TechRadar

04

Securing the Quantum Age

Palo Alto Networks

Content brought to you by paloalto NETWORKS

Quantum-Ready Security: The Time to Act is Now

Harvest now, decrypt later. That's the threat posed by the impending arrival of quantum computing. But there's a lot of confusion surrounding quantum. Is it truly today's problem, or tomorrow's? And if the former, where can you get started and what should your priorities be for making sure your data remains secure?

From the relentless rise of ransomware to the ongoing boom in AI, the cyberthreat landscape already seems vast and overwhelming – and that's without the full, widespread adoption of quantum technologies.

But preparedness is key – taking steps today to secure what's coming tomorrow will position your organization for success. From migrating legacy systems to identifying critical data across complex multi-cloud environments, there are challenges you can already start tackling.

In this trends report, educate yourself about the quantum reality by learning what's actionable in the here and now so that you can start to demystify the task of cybersecurity in a post-quantum world.

01

Cyber Resilience in the Post-Quantum Era: The Time of Crypto-Agility

Tim Zonca | TechRadar

We are at a tipping point for quantum computing, which is on the verge of becoming a reality.

While its potential is tantalizing, it also represents an unprecedented threat to the traditional data security infrastructure and the cryptographic algorithms that protect it. Post-quantum cryptography – algorithms designed to be secure against classical and quantum computer attacks – is the response.

Quantum computers exploit the principles of quantum mechanics to solve complex problems that classic computers cannot feasibly tackle. Quantum computers use the principles of quantum mechanics to process information in a way that uses qubits, which can exist in multiple states, as opposed to normal computers, which only use “zeros” and “ones”. This creates an exponential scale, which is what gives them their computational power.

Of particular concern is their ability to crack widely used public key encryption algorithms such as RSA and ECC (elliptic curve cryptography). By the time a sufficiently powerful quantum computer becomes available, these encryption methods, which protect virtually all current digital communications, will be obsolete.

The date when cryptographically-relevant quantum computers will appear remains uncertain: estimates range from five to 10 years. However, the risk is immediate due to the “harvest now, decrypt later” attacks that are already taking place, especially for data with a longer lifetime.

If an organization retains sensitive data for the long term, such as financial information, personal data or even trade secrets, this represents a significant and growing risk.

What is at stake is nothing less than the most valuable digital assets: intellectual property, private and sensitive data, authentication systems and secure communications.

The financial, operational and reputational damage from such exposures could be catastrophic, and unavoidable without proactive measures.

The risk is immediate due to the “harvest now, decrypt later” attacks that are already taking place, especially for data with a longer lifetime.

What is post-quantum cryptography?

Post-quantum cryptography (PQC) refers to cryptographic algorithms designed to be secure against attacks by classical and quantum computers. These algorithms are based on mathematical problems that remain difficult to solve even for quantum computers.

In 2024, the National Institute of Standards and Technology (NIST) published its first set of standardized post-quantum cryptographic algorithms, including CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+ and FALCON. In March 2025, NIST selected a new algorithm, Hamming Quasi-Cyclic (HQC), which will serve as a backup to the existing Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) algorithms recommended by FIPS 203 to protect against quantum attacks.

HQC is based on error-correcting codes, a concept that has been fundamental to information security for decades. Unlike ML-KEM, which relies on structured networks, HQC’s unique mathematical basis offers a robust alternative that can help combat the potential threats posed by future quantum computers. This shift in mathematical approaches is crucial for maintaining the integrity of encrypted data.

The time for change is now

The time when currently encrypted data can be decrypted using quantum technology is closer than many people think. However, while most organizations are actively working on cyber resilience strategies, including their core IT infrastructure and components of the supply chain, the risk to quantum computing is not as widely considered.

Changing cryptography in a complex IT environment is not something that can be done overnight. It can take years, especially for large organizations with complex IT environments. Historical precedent shows that major cryptographic transitions typically take 5-10 years to complete.

While most organizations are actively working on cyber resilience strategies, including their core IT infrastructure and components of the supply chain, the risk to quantum computing is not as widely considered.

Beginning the transition

To begin a transition to post-quantum cryptography, a number of steps must be followed:

1. **Cryptographic inventory:** Not all data is equally important, and not all data needs to be encrypted in the same way. It is therefore necessary to identify where cryptography should be used in the digital heritage. This should include the most sensitive data, applications, networks, identity systems, and third-party connections.

2. **Risk assessment:** Given the cost of post-quantum cryptography, it makes sense to prioritize protecting the most sensitive data rather than trying to protect everything. Evaluate your data in terms of its sensitivity and longevity. Information that must remain confidential for more than five years should receive immediate attention. For less sensitive data, standard encryption methods will suffice in keeping it secure.

3. **Crypto-agility implementation:** Being crypto-agile – having the ability to switch between different cryptographic algorithms in response to new threats – will be essential in the post-quantum era. Develop frameworks that allow you to quickly replace cryptographic algorithms without the need for extensive system redesign. Crypto-agility also requires employee training, so invest time and resources to bring your employees on this journey with you.

4. **Prioritized migration:** Start with your most sensitive systems and data, particularly those that protect intellectual property or personally identifiable information.

5. **Supplier engagement:** Confirm that all suppliers in your ecosystem are aligned with emerging standards to ensure end-to-end protection and agility.

In summary

By starting your post-quantum transition today, you can help protect your organization's most valuable data as we enter the quantum era. The alternative is to wait for quantum computers to break existing encryption – by then, it will be too late for data that has already been compromised. The future is quantum and the time to future-proof your data is now.

02

The Clock is Ticking on AI Security in a Quantum World

Kolawole Samuel Adebayo | Forbes

Quantum threats are accelerating fast. Experts note that if AI infrastructure isn't secured soon, the consequences could be irreversible.

AI now runs in courtrooms, hospitals, airports, banks and several industries, becoming the crown jewel of many modern enterprises. However, protecting these AI systems in a quantum future is becoming increasingly difficult.

Somewhere between the optimism of generative AI and the acceleration of quantum computing is a growing risk that few organizations are addressing today. While many worry about adversarial prompts and model hallucinations, experts say those are the least of our problems.

David Harding, CEO of *Entrokey Labs* — a cybersecurity firm building quantum-resistant key infrastructure — warned that the real risk lies in how AI systems handle sensitive data. He argued that AI systems, and the massive volumes of sensitive data they ingest, may soon be the first victims of quantum-enabled cyberattacks. And most companies are walking into that future blind.

The quantum threat isn't theory anymore

Earlier this year, Nvidia CEO Jensen Huang *described quantum computing* as reaching "an inflection point." While that statement sparked interest among investors, its implications for cybersecurity — particularly for AI-driven systems — haven't fully sunk in. As researchers push closer to building scalable quantum machines, long-standing encryption protocols such as RSA and ECC could be broken, making previously secure data fair game.

In other words, the data feeding your AI today may be tomorrow's biggest liability. This isn't some distant sci-fi scenario. The groundwork has already begun. Nation-state actors are believed to be stockpiling encrypted data using what's known as a "harvest now, decrypt later" strategy. Think of it like thieves stealing locked safes today knowing they'll get the keys tomorrow.

Once *quantum machines* become powerful enough, they could retroactively decrypt troves of corporate secrets, defense communications and medical data, including everything passed through AI models today.

"Any electronic data is at risk from harvest now, decrypt later if it is not using digital keys resistant to today's AI attacks and near-term quantum attacks," said Harding. "Several countries including Russia, China, Iran and North Korea have well over 100,000 individuals solely focused on hacking our systems. Add automation into the mix, and the scale becomes nearly unmanageable."

Quantum threatens all digital systems, but AI amplifies the risk. These models don't just generate content — they ingest patient records, financial models, intellectual property and legal data. In autonomous systems, they make decisions. In others, they write code and trigger workflows. That puts entire AI pipelines — from training data to deployed agents — directly in the crosshairs.

"Quantum and *AI-safe encryption* has the same level of importance as the foundation of a building," explained Scott Streit, Entrokey Labs' chief scientist. "Without it, the structure collapses. There'd be no protection for customer data, IP or communications. In national security, satellites or precision weapons could be taken over."

Falling behind the curve

Despite these risks, many enterprises still treat quantum computing as a future problem — something to solve by 2030. The U.S. National Institute of Standards and Technology (NIST) has laid out a path for *adopting quantum-safe cryptography* by 2035. But according to Harding, that timeline no longer reflects how fast both AI and quantum capabilities are evolving.

“The timeline is increasingly out of step with the pace of AI and quantum advancements,” said Harding. “Some believe AI is already breaking into encryption systems.”

And yet, most organizations continue to treat quantum-readiness as a long-haul IT project, involving years of consultations, infrastructure upgrades and vendor reviews. Harding refers to this pattern as “cyber inertia” — an outdated playbook for a much faster threat.

“We’re trying to solve a smarter threat with outdated answers,” Harding said. Streit added that “AI can already create math that top mathematicians can’t explain,” arguing that “the only way to win is by using AI to secure AI.”

To make matters worse, regulatory frameworks haven’t caught up. Neither the EU AI Act nor *NIST’s AI Risk Management Framework* say much about defending AI systems against quantum cryptographic threats, leaving a critical vulnerability unaddressed at the policy level.

“AI can already create math that top mathematicians can’t explain,” arguing that “the only way to win is by using AI to secure AI.”

What's at stake

The financial fallout from a breach caused by quantum decryption is hard to estimate. But the principle is simple: What's considered secure today may not be tomorrow. That includes confidential model outputs, internal prompts, logged agentic decisions and sensitive metadata. Any of it could be exposed or tampered with.

"Think about how we respond to weather warnings," Harding said. "If there's even a 10% chance of a tornado, you don't wait. You get to shelter."

He added that this level of risk isn't something CISOs can handle alone. "Quantum is a boardroom issue now — not just an engineering one. The scale of impact makes Y2K look like a warm-up act."

"Quantum is a boardroom issue now — not just an engineering one. The scale of impact makes Y2K look like a warm-up act."

If trust fails, AI fails

While companies double down on AI performance, many remain dangerously naive about the risks embedded at its roots. As Harding put it, "The question is no longer whether quantum will impact AI systems, but how quickly organizations can adapt before it does."

AI security depends not just on encryption, but on anticipating how fragile the entire ecosystem becomes when that encryption fails. If attackers can retroactively decrypt, reroute, or manipulate those systems, the blow to public confidence could rival or exceed any previous cyber event.

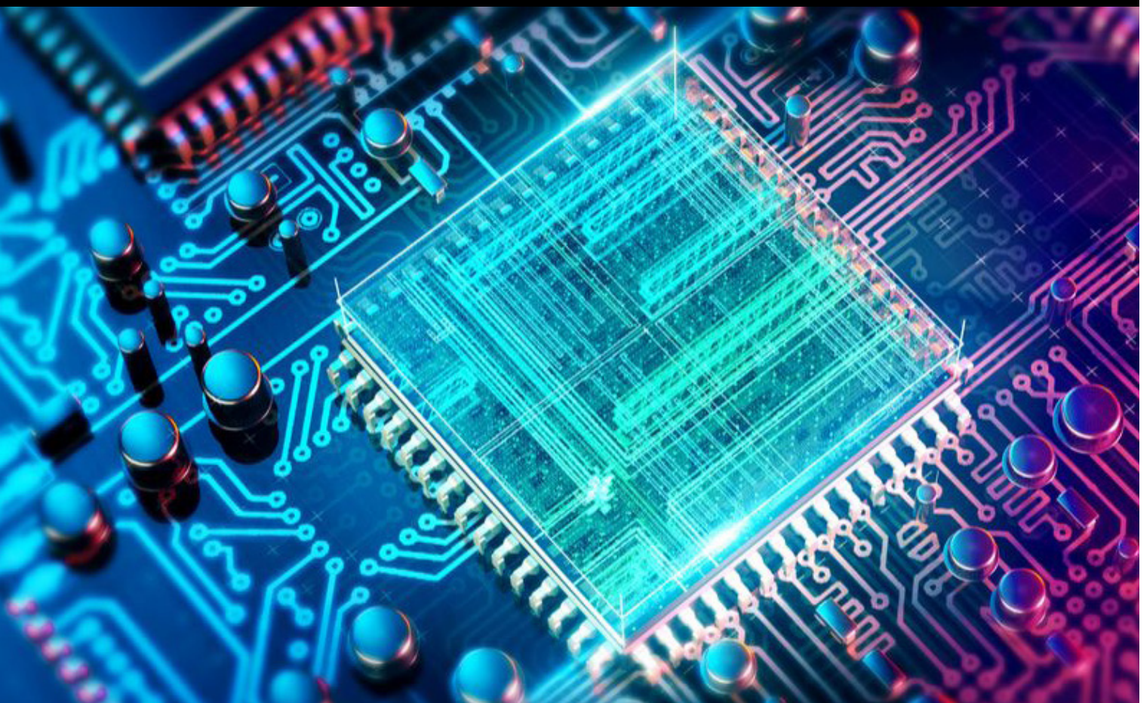
Trust is what gives AI its power. Lose that, and even the smartest models would collapse.

"We've built an entire era of decision-making on architectures that might be more fragile than we thought," Harding said. "While companies chase optimization, adversaries are chasing the keys."

03

Preparing for a Quantum-Safe Future Should Begin Today

Avishai Sharlin | TechRadar



Data is today's premier strategic asset. With quantum computing opening the floodgates for a new age of cyber threats, post-quantum cryptography (PQC) must become a cornerstone of security.

Preparing for a post-quantum future will require a significant time investment, one that business leaders cannot afford to put off.

They must give themselves time to refactor all their applications to ensure no measures slip through the cracks.

The future commoditization of quantum computing

Transitioning to PQC is an imperative. Almost all our technologies rely on cryptography to protect critical data in software. Once quantum cryptography falls into the hands of malicious actors, all this data will essentially be exposed.

It is only a matter of time before this happens. Like any other new technology, it will initially be expensive and difficult to acquire. As more players enter the market, this technology, too, will become commoditized.

AI followed a similar path. Before the launch of widely available LLMs like ChatGPT, AI was bound to niche technological applications or available only to researchers. However, with GenAI models rising in popularity, AI capabilities became widespread, becoming accessible to malicious actors.

We can imagine a similar fate for quantum computing, where the ramifications are a matter of survival for businesses. It will be that much easier for malicious actors to acquire these capabilities.

Regulatory standards

Authorities all over the world are taking note of the quantum risk, and the competition to become the leader in standard-setting is heating up. While the regulatory landscape is still in its infancy, the UK, US, and EU have made significant developments recently in laying the groundwork for an approach.

The UK's National Cyber Security Centre (NCSC) recently asked organizations to transition to quantum-resistant encryption methods by 2035.

The EU launched its Quantum Europe Strategy, taking a top-down approach to regulation, aiming to coordinate member states.

The US Department of Commerce's NIST officially finalized the first set of encryption algorithms designed to withstand potential threats from quantum computers.

This means organizations need to stay vigilant to anticipate where regulation and standard-setting are headed. With competing approaches and interests, it will be important to find common ground and build compliance into preparations for PQC.

Most notable from existing standards is NIST's proposed set of PQE algorithms. This is a good starting point toward global PQC standards and offers a valuable starting point for organizations looking to explore PQC options.

These are the new standards for encryption in PQC. Experimenting with these algorithms and developing processes and capabilities to transition to PQC will put businesses in a strong position for navigating standards and regulations.

The scale of the transformation required to be quantum-safe cannot be understated. Adopting quantum-resistant algorithms is technically complex and time-consuming. Organizations will need to refactor all their applications.

The time to act is now.

The adoption of Post-Quantum Encryption (PQE), as published by NIST, requires organizations to experiment and test—often many times—and iterate a procedure throughout the company.

First port of call: Excellence from within

It is essential to understand the necessary skills, processes, and evaluation frameworks for PQC are still being developed.

Yet the adoption of Post-Quantum Encryption (PQE), as published by NIST, requires organizations to experiment and test—often many times—and iterate a procedure throughout the company.

An intelligent way to align company resources and stakeholders is by establishing a Center of Excellence (CoE) to lead implementation.

What would a CoE look like? Centers of Excellence are forums where leaders from across the organization can meet to collaborate and strategize for the post-quantum transition.

They can also audit current applications and infrastructure for clarity and direction, gauging where the weak points lie, where dependencies are heaviest, and which processes will ease the adoption of PQE.

To start, leaders must assess the scale of the upgrade across their systems. This involves auditing current services and applications to see which rely on cryptography and identifying the programming languages (e.g., Java), operating systems, and frameworks (e.g., Spring) that will be affected.

It also includes considering available mitigations—for instance, RHEL 10 is the first Linux OS to fully support PQC. From there, they can set priorities for adopting PQC.

Importantly, Kubernetes, a core tool for managing containerized applications, has already taken a proactive step to support PQC in a hybrid approach ahead of time - showing that the industry is taking the threat of quantum computing and the need for PQC very seriously.

This update sets a strong precedent for other technologies to follow suit in ensuring their readiness for the post-quantum era. This proactive move is a prime example of how organizations should think ahead in adopting quantum-safe solutions before the full advent of quantum capabilities.

Updating entire IT infrastructures is a mammoth task for the industry. It requires updates not only to legacy systems but also to modern software that is not quantum-safe.

To increase the complexity, it isn't solely an IT problem. PQC cuts across legal, compliance, product, procurement, and customer boundaries. A quantum Center of Excellence demands cross-functional leadership roles, not simply technologists.

Updating entire IT infrastructures is a mammoth task for the industry. It requires updates not only to legacy systems but also to modern software that is not quantum-safe.

The quantum class of tomorrow

Across much of the technology industry, the necessary IT skills are scarce. An estimated 44% of businesses have skills gaps in basic technical areas; quantum is no exception. But CoEs have the added benefit of upskilling workers, paving the way for future talent.

They set guardrails from structured training across the company, sifting out gaps in knowledge and creating a focused environment for learning emerging technologies and methods, while offering hands-on experience, mentoring, and certification opportunities.

An estimated 44% of businesses have skills gaps in basic technical areas; quantum is no exception. But CoEs have the added benefit of upskilling workers, paving the way for future talent.

The path to a quantum-safe future

Advancements in quantum technology are rapidly closing the gap between research and real-world applications. Industry leaders like Microsoft, Google, and IBM have already unveiled quantum chips, signaling that practical adoption is closer than many anticipated.

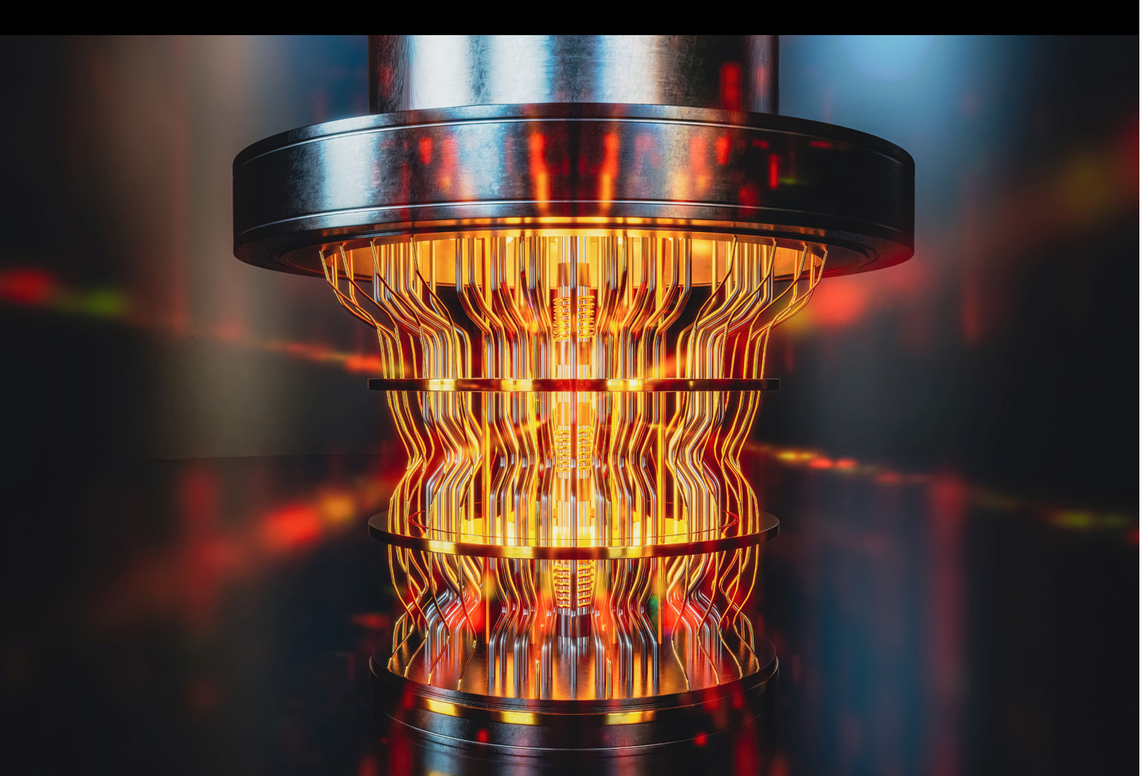
Rushing the transition to PQC without careful planning risks overlooking critical technical, operational, and regulatory considerations. A successful shift demands early action, strong leadership, and collaboration across departments.

Centers of Excellence (CoEs) can play a pivotal role in guiding organizations through this complexity, ensuring strategies are executed effectively. Those who take the lead in achieving quantum readiness today will be best equipped to thrive in a future defined by secure digital innovation.

04

Securing the Quantum Age

Richu Channakeshava, Sean Morgan
| Palo Alto Networks



New Cryptography Inventory Tool, Quantum-Optimized Firewalls and PAN-OS 12.1 Enable Quantum Readiness

The cybersecurity landscape is rapidly shifting due to a risk that's quietly brewing in the background: the race to achieve quantum supremacy. Quantum computing has long promised to redefine what's possible in technology, with its ability to solve complex problems exponentially faster than classical computers. This technological breakthrough promises many benefits likely to unlock trillions in economic value but will also introduce major new risks to the cryptographic foundations of modern cybersecurity. Despite this significance, quantum is still often dismissed as a problem too far away to worry about.

That's changing with the convergence of AI and quantum computing. Researchers are now leveraging AI to reduce some of the key barriers to quantum computing, like automating qubit error correction and optimizing quantum algorithms. This means cryptographically relevant quantum computing (CRQC) – the point at which quantum systems can break today's public key cryptography – could arrive sooner than the industry initially projected. McKinsey (2024) predicted a CRQC could break the most common public-key encryption algorithms as soon as 2027, while Gartner (2025) predicts that most conventional asymmetric cryptography would be unsafe to use by 2029.

Governments around the world have taken notice, developing new national quantum readiness strategies, including requirements to migrate to new quantum resistant Post-Quantum Cryptographic (PQC) standards, like those developed by the United States National Institute of Standards and Technology (NIST). Organizations are also experimenting with solutions beyond PQC migration, adopting technologies like Quantum Random Number Generation (QRNG) and Quantum Key Distribution (QKD) to build additional resilience to unforeseen computational advancements.

These emerging quantum readiness strategies have another common thread: emphasizing the critical role technology providers can play to proactively lead in the quantum era. At Palo Alto Networks, we're meeting this moment by announcing a comprehensive suite of new quantum security capabilities as part of PAN-OS 12.1 Orion and our new quantum-optimized fifth-generation Next-Generation Firewalls (NGFW).

At Palo Alto Networks, we're meeting this moment by announcing a comprehensive suite of new quantum security capabilities as part of PAN-OS 12.1 Orion and our new quantum-optimized fifth-generation Next-Generation Firewalls (NGFW).

These capabilities will empower organizations globally, across government and critical infrastructure, to accelerate their quantum readiness in alignment with emerging global and regional standards. Here is how our new capabilities can help your organization meet some of the fundamental imperatives of quantum readiness:

Discover — Conducting Automated Cryptographic Inventories

- **Challenge:** Establishing foundational visibility of your organization's cryptographic usage is often cited as the best first step to kick-start quantum readiness. But legacy cryptographic inventory technologies have been insufficient, providing an incomplete and static snapshot of cryptography usage, failing to connect cryptography to sensitive data, and unable to empower users to take remediation action in real-time.

- **Solution:** Palo Alto Networks announced Strata Cloud Manager's *'Quantum Readiness'* view and a forthcoming *'Cryptographic Inventory'* insights dashboard to help you prepare for the quantum era. Organizations can gain visibility and take control of their cryptographic risk posture across users and applications from a single management interface.

With Quantum Readiness view, we're introducing several capabilities:

1. **Inventory** and assess cryptography usage as secure, weak or vulnerable.
2. **Validate** compliance with a range of government standards and regulations.
3. **Remediate** and upgrade to PQCs through an inline workflow.

Deploy — Migrating to PQC-Enabled Technologies

- **Challenge:** Once an organization establishes visibility of its cryptographic risk posture through inventorying, then migrating high-risk systems to new PQC standards is another critical step in quantum readiness. This action is particularly time sensitive for organizations that hold data with long-term value. Adversaries are already conducting 'harvest now, decrypt later' attacks with the intent to decrypt once a quantum computer becomes available. Collaborating with technology partners who are proactive and transparent about their products' supportability with PQC standards is a critical part of quantum readiness.
- **Solution:** PAN-OS 12.1 Orion, running on our fourth-generation and newly announced fifth-generation NGFWs, now includes support for all NIST standard algorithms: FIPS 203: ML-KEM, FIPS 204: ML-DSA, FIPS 205: SLH-DSA and other prestandard algorithms – HQC, Classic McEliece, BIKE, Frodo. PAN-OS 12.1 Orion also delivers Quantum-safe site-to-site VPN Tunnels and SSL/TLS sessions to protect against more immediate "harvest now, decrypt later" attacks.

Our implementation is focused on providing a more seamless transition to quantum-safe algorithms with prioritization:

1. **Global interoperability** through alignment with international standards and regional requirements, such as those in the European Union, United Kingdom, United States, Australia, India and more.
2. **Cryptographic agility** through flexible support for multiple standard and prestandard algorithms.
3. **Hybrid algorithms** through support for concatenation of classical and post-quantum algorithms for enhanced security in encryption.

Deploy — Adopting Quantum-Optimized Hardware

- **Challenge:** Given the significant compute and memory requirements for hybrid and cryptographically agile implementations of PQC, not all IT systems will be able to be made quantum-ready through software upgrades alone. Hardware modernization will be necessary, and organizations will need to be judicious to ensure they're not simply replacing legacy IT with more legacy IT for the quantum era.

- **Solution:** Palo Alto Networks just announced our fifth-generation NGFW which are performance optimized with a suite of additional capabilities to future-proof your investment for quantum security defense-in-depth. Our PA-5500 Series NGFW is Quantum Optimized with up to 256 cores of compute and hardware acceleration to process encryption at scale. With network packet processing powered by the FE400 ASIC, the PA-5500 series NGFWs support 400 Gbps interfaces to meet the needs of modern data centers.

Hardware modernization will be necessary, and organizations will need to be judicious to ensure they're not simply replacing legacy IT with more legacy IT for the quantum era.

Many organizations are seeking additional methods to build quantum-resistant infrastructure as either a fallback mechanism or a primary solution.

Deploy — Enabling Layered Defense through PQC and Quantum-Key Distribution Support

- **Challenge:** While PQC migration has been the primary focus for securing digital communications against future quantum computer attacks, there is no guarantee around the long-term efficacy of the PQC standards as they just begin to undergo large-scale global testing. To address this risk, many organizations are seeking additional methods to build quantum-resistant infrastructure as either a fallback mechanism or a primary solution.

- **Solution:** With PAN-OS 12.1, Palo Alto Networks is announcing support for ETSI 014 protocol integration, leveraging Quantum Key Distribution (QKD) capabilities to establish cryptographic keys resistant to unforeseen computational advancements. With the support for both PQC and QKD in PAN-OS 12.1, we provide organizations with a hybrid and agile approach, offering a robust, multilayered security posture, to bolster resilience in an evolving and unpredictable quantum landscape.

Protect — Secure Legacy Applications and IoT/IT Infrastructure with Cipher Translation Proxy

- **Challenge:** Organizations face a difficult balance between efficiently migrating systems to PQC while also prioritizing near-term operational continuity for their organization. This challenge is particularly acute for organizations with high levels of dependency on legacy systems, such as in manufacturing and other operational technology (OT)-dependent environments.

- **Solution:** With PAN-OS 12.1, we introduce a "cipher translation proxy" that offers a critical bridge for web applications that cannot be migrated to PQC and must be protected. This intelligent proxy acts as an intermediary, seamlessly translating classical cryptographic communications into quantum-safe ones and vice versa. This capability allows organizations to bolster their security against future quantum threats without immediately overhauling legacy systems, ensuring continuous operations, data protection and achieving PQC compliance as they strategically transition their entire infrastructure.

The surge in global attention around quantum computing-related risks should be a wake-up call for any organization across the public and private sector seeking to accelerate their own quantum readiness. It should also be a call to action for all technology providers to ensure they're doing their part to proactively develop technologies prepared for the unique risks of the quantum era.

At Palo Alto Networks, we're answering that call by delivering advanced, integrated solutions that offer the visibility, agility, as well as remediation capabilities essential for true quantum readiness. We also recognize that public-partnership is critical in this global effort, which is why we're also embracing a leadership role within the broader ecosystem — establishing a QRNG Open API Coalition and as proud partners at NIST's Migration to Post Quantum Cryptography project.

As attention shifts to this next significant cybersecurity challenge, Palo Alto Networks remains committed to lead through both technological innovation and partnerships, as a strategic partner in the global pursuit of quantum readiness.

Want to learn how to safeguard your enterprise from post-quantum threats?
Hear from our experts on how to be quantum-ready.

As the global AI and cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.