VENARI SECURITY

Whitepaper

Post-Quantum Cryptography: A Revolution or Just the Next Upgrade?

Mark Slater

Director Channel Sales

The evolution of secure communication protocols is a story of constant adaptation. We've seen this journey through the decades:

- IPSec VPNs safeguarded network traffic.
- SSL emerged, evolved, and ultimately handed over to TLS.
- TLS 1.0, 1.1, 1.2, and now 1.3 were deployed as part of a natural progression to address vulnerabilities and improve performance.

Now, Post-Quantum Cryptography (PQC) is being positioned as the next frontier—but is it truly a radical departure requiring a ground-up overhaul, or is it simply the latest phase in our upgrade lifecycle?

Evolution or Revolution?

For decades, organisations have been forced to adapt to the relentless pace of cyber threats. Each iteration of security protocols demanded careful deployment, testing, and integration into existing systems. PQC feels like another chapter in this familiar playbook, yet its positioning suggests otherwise. The key difference? PQC is a response to an entirely new class of threats posed by quantum computers.

The question remains: Do we need to start afresh to deploy PQC, or can we treat it as an extension of our existing cryptographic infrastructure?

The Quantum Horizon: A Call for Urgent Attention

While discussions around Post-Quantum Cryptography (PQC) might feel futuristic, the underlying challenge—the rise of quantum computing—is rapidly moving from theoretical to practical. This isn't simply a niche concern for tech enthusiasts; it's a seismic shift that has the potential to reshape the entire cybersecurity landscape, demanding our immediate and focused attention.

The sheer power of quantum computers to break today's commonly used encryption is not a matter of "if," but "when." Experts predict that by 2034, the Post-Quantum Cryptography market will surge to a staggering $17.69 billion, a dramatic increase from $356.4 million in 2023. This exponential growth, projected at a CAGR of 41.47%, is a reflection of the imminent and very real threat to our digital world, signalling a transformative moment in cybersecurity.

The implications of this transformation are far-reaching. The information we depend on every day for critical functions—from financial transactions to healthcare records and national security communications—is becoming increasingly vulnerable to quantum-powered decryption. This is not a future concern; the very data being encrypted using currently standard protocols is at risk from being retroactively decrypted once quantum computing becomes a viable reality. This is why governments, major industries, and research labs are accelerating investment in quantum-resistant solutions, driven by a proactive approach to the looming threat.

What Makes PQC Different?

Unlike previous upgrades, PQC isn't just about efficiency or fixing vulnerabilities. It's about preparing for an era when quantum computers might make current encryption obsolete. However, PQC solutions are being developed with backward compatibility in mind, particularly for hybrid models combining quantum-resistant algorithms with traditional cryptographic systems.

This opens the door for PQC to be integrated without tearing down existing architectures.

Lessons from History: Upgrade Fatigue

Think back to the transition to TLS 1.3. Organisations grappled with implementation challenges, ensuring compatibility with legacy systems while improving their overall security posture. The journey wasn't without its hurdles, but it followed a pattern:

1. Standardisation.
2. Integration with existing infrastructure.
3. Gradual deployment.

PQC can follow a similar trajectory if we approach it pragmatically. By embedding PQC algorithms into current frameworks, such as in hybrid models or quantum-resistant VPNs, organisations could ease into adoption without disrupting their operations.

The Call to Action: Be Ready, Not Fearful

While PQC represents an upgrade in security, it also brings a fundamental shift in mindset. The quantum threat may seem distant, but preparation is key. Organisations should:

1. Start inventorying critical systems that rely on vulnerable cryptographic protocols.
2. Plan for hybrid solutions to transition gradually.
3. Engage with vendors and industry bodies to stay informed on PQC standardisation efforts.

PQC doesn't have to be a "new start." Instead, it can—and should—be treated as part of the natural evolution of security protocols. What's critical is that we recognise it for what it is: not a choice, but a necessity.

The Next Iteration

PQC isn't a break from tradition; it's the next iteration in the ongoing journey of cybersecurity. If TLS 1.3 taught us anything, it's that change is inevitable—and manageable. With the right strategy, PQC can be deployed as seamlessly as the upgrades that came before it.

The key to success lies in preparation, and that starts with understanding what you already have. Here at Venari Security, Inventory Discovery is what we do. By providing visibility into your cryptographic assets, we help organisations identify vulnerabilities, evaluate readiness, and ensure a seamless transition to quantum-safe cryptography.

So, is PQC a revolutionary new start? Or just another upgrade? Perhaps it's both—but either way, the time to prepare is now.

What are your thoughts? I'd love to hear how your organisation is approaching the quantum challenge.

Bridge your knowledge gap.
Visit: www.venarisecurity.com

Venari Security Ltd.

16 Great Queen Street, London,
WC2B 5AH, United Kingdom
+44 (0)20 7294 7749
info@venarisecurity.com

About Venari Security

Venari Security provides organisations with advanced visibility into their encrypted attack surface, ensuring regulatory compliance and privacy adherence through our cryptographic discovery tool.

Our focus is on crypto agility which helps you assess both external and internal cryptographic risks, preparing your business now and for the quantum future.