Venafi

InfoSec's Guide to Post-Quantum Readiness

Learn why now is the time to begin preparing for radical changes in cryptography

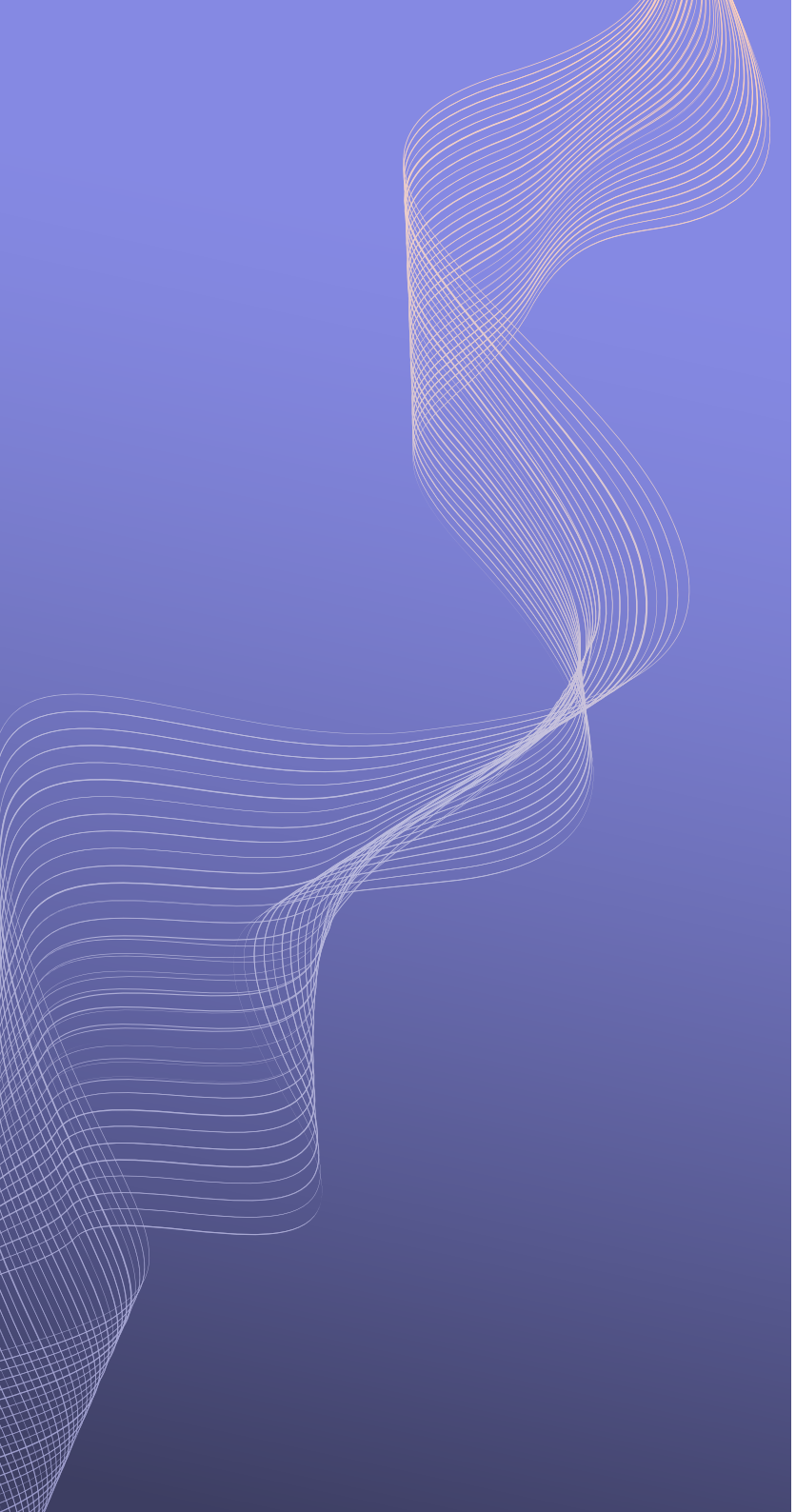
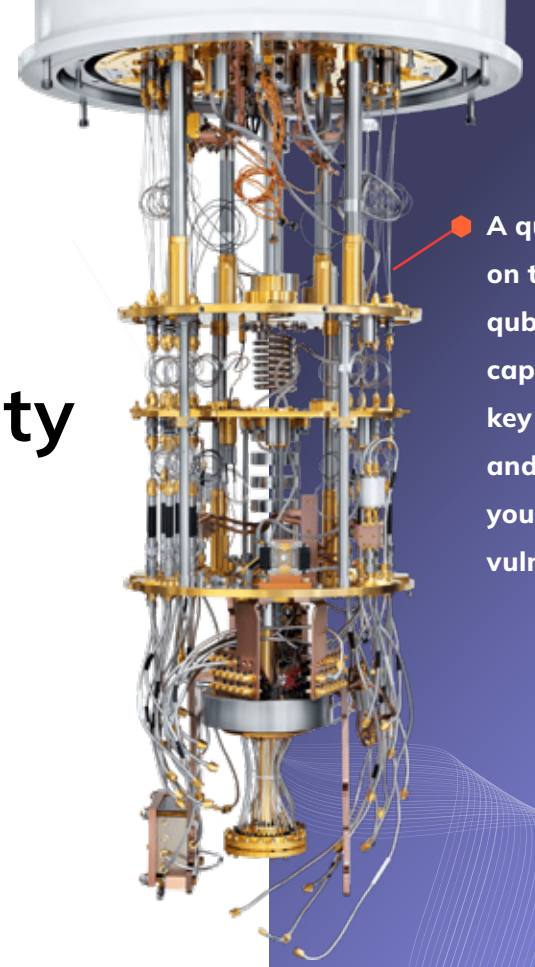


Table of Contents

Quantum computing: a game changer for society AND security

Quantum computers offer significant advantages to society, far outperforming their classical counterparts in areas like pharmaceutical research, financial modeling, and climate change predictions. And although we can't wrap our heads around the full impact quantum computers will have on our world, one thing's absolutely certain: **they'll bring enormous cybersecurity risks.**

That's why staying on top of recent developments in post-quantum cryptography (PQC) and developing a plan for migrating to quantum-resistant encryption is critical to ensuring your business doesn't just survive—but thrives—in a post-quantum world.



A quantum computer running on the right number of ideal qubits (approx. 4,000) is capable of breaking public-key cryptography like RSA and ECC encryption, leaving your otherwise secure data vulnerable to attack and theft.

Quantum acceleration ignites

Quantum computers may not be strong enough to obliterate today's cryptographic algorithms yet, but the industry made significant strides in 2023. And it's picking up momentum.

Developments related to quantum computing arose on an almost-monthly basis in 2023:

January

Memo on Improving Security of DoD, Intelligence Community focuses on preparing for quantum-resistant protocols

March

National Cybersecurity Strategy released, stressing quantum preparation as a strategic objective for a resilient future

Cloud Security Alliance sets Q-Day countdown clock for 2030

May

Memo on Promoting US Leadership in Quantum Computing while Mitigating Risks to Vulnerable Cryptographic Systems released

July

NIST Publishes First Draft Standards for Quantum-Resistant Cryptography

September

NSA announces Commercial National Security Algorithm Suite 2.0, proclaiming everyone should work toward quantum-resistant algorithms

October

Atom Computing becomes first to reach 1,000 qubits

November

OMB issues memo urging agencies to begin post-quantum transition

December

IBM's introduces Condor processor, boasting 1,121 qubits

The road to Q-Day

Many quantum experts, including the Cloud Security Alliance, predict Cryptographically Relevant Quantum Computers (CRQCs) will arrive in 2030-2033. But with developments happening at a higher velocity, might we see a shorter timeline? What does the journey to Q-Day look like?

Important!

The countdown to Q-Day isn't being done on a doomsday device. With careful preparation and planning, your company can be ready for tomorrow's problems—today.

2024-2026

You can expect regulatory bodies like NIST to standardize the first quantum-resistant algorithms. In the following 1-2 years, certified libraries will begin implementing PQC programs, and standardization bodies around the world will update their own protocols with NIST's algorithms.

2027-2029

A huge vendor push will occur, as technology companies use NIST-approved algorithms to update program protocols and implementations.

2030-2033

Q-Day arrives! Experts predict a quantum computer will be able to break present-day cybersecurity infrastructure at this time.

Why should I be concerned about quantum computers already?

The arrival of CRQCs may be a few years off, but industries who handle confidential, private, or customer information should start planning sooner, rather than later. If you're not in an industry like finance, healthcare, or public services, the situation is less dire (for now), but it's still something to be aware of. And it's not a bad idea to start today—encryption shifts, as historical evidence shows, take a lot of time.

Regardless of your industry, you'll still need to solve for the same problems.

95% **Of organizations surveyed aren't ready for a world with quantum computers—and half say they're not yet concerned.**

SOURCE: Quantum-Proofing Your Data: Are You Ready for the Future of Cryptography? >>

Steal now, decrypt later attacks:
Threat actors are already harvesting encrypted data, storing it, and planning to decrypt it when CRQCs become commercially available.

Unauthorized code execution:
Without a resilient code signing operation, internal software faces a greater risk of ransomware, malware, zero-day exploits, and other tampering.

TLS protocol transition:
To deny others the ability to read, modify, or intercept data—or impersonate your business—TLS protocols need to be transitioned to NIST-approved, quantum-resistant algorithms.

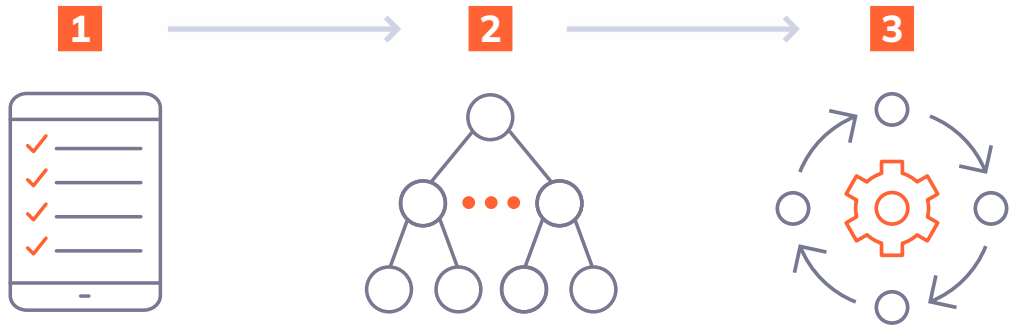
Active protection of data and code in use:
Data and code that's actively being accessed and processed must also be protected.

What do these challenges have in common?

Solving them relies on a bedrock of machine identities, and managing those identities requires robust visibility and automation across varying types, like TLS/SSL, code signing, SSH, SPIFFE, SVID, and mTLS.

Your 3 steps to quantum victory

Standardization bodies like NIST, ETSI, ENISA, AIVD, and BSI all recommend a 3-step approach for migrating from traditional to post-quantum cryptography. And it all hinges on having a comprehensive machine identity management system.



01 PQC Diagnosis

02 Planning the Migration

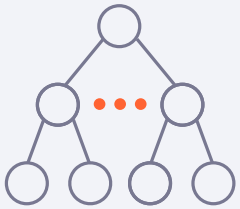
03 Execute the Migration

01 PQC Diagnosis

Your first step is to inventory all machine identities, the protocols, and the applications that use them.

Pro Tip

If you don't have this intelligence in place, you won't be able to move to a post-quantum enabled infrastructure. Ensure your machine identity management platform provides these capabilities.



02 Planning the Migration

Next, you should plan, prioritize, and test migration for critical machine identities, and all associated applications, to protocols or schemes that leverage PQC algorithms.

Pro Tip

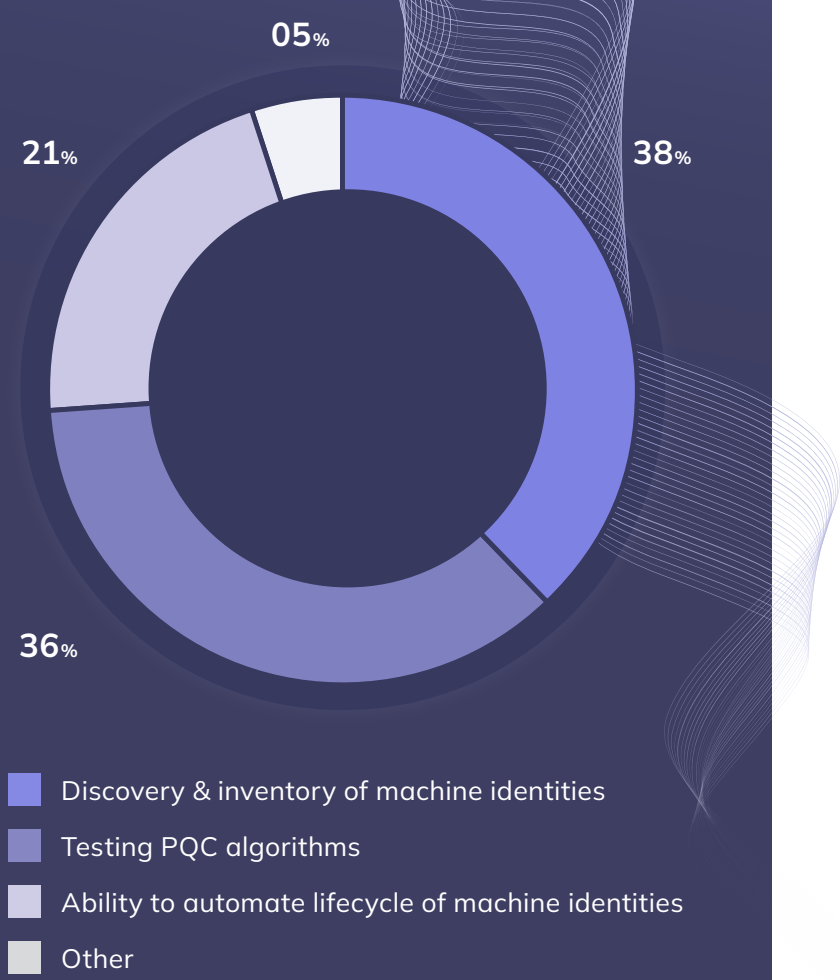
How you prioritize your plan of attack is important and will differ from business to business. You also want to make sure your machine identity management platform provides the crypto-agility you need to migrate to PQC, as well as the ability to test hybrid certificates and PKI solutions today.

03 Execute the Migration

Don't you love it when a plan comes together? This is where you decide on timing and execute the migration of critical machine identities and associated applications.

Pro Tip

To ensure successful execution, you'll need to migrate machine identities iteratively. You may find it helpful to work alongside an experienced machine identity management partner, as they can smoothly guide you through the transition process.



InfoSec's largest concerns

According to a survey conducted during the online discussion "Quantum-Proofing Your Data: Are You Ready for the Future of Cryptography?", Information Security professionals are most concerned with the discovery and inventory of existing machine identities, as it relates to PQC readiness.

Expert insights

We asked our resident PQC expert, Faisal Razzak, to weigh in on these numbers, which he deems unsurprising. Most companies are currently in the diagnosis stage, so it makes sense that most are worried about building a comprehensive inventory of machine identities.

Razzak also emphasized that, though automation is a lower concern for many today, it's still a critical piece of the puzzle.

"The scale of machine identities involved in a PQC migration will be massive, and automation a necessity. It's also vital for assuring crypto-agility, which enables your machine identity management to turn on a dime in case of large-scale events, such as widespread cryptographic vulnerabilities.

Faisal Razzak
Group Manager, Post Quantum & Secure Software Supply Chain Initiatives
Venafi

AI's impact on the PQC timeline

Software is eating the world, and if we've learned anything from the past year of AI-related developments, AI is eating that software. The scale of the shift to post-quantum is already set to be huge, but if you throw AI into the mix, that scale multiplies exponentially.

Advancements in AI research also have the potential to speed up PQC-related research. As more AI/ML experimentation occurs, more threat vectors will emerge—perhaps even impacting otherwise secure cryptographic algorithms.

And as the world learns more about AI infrastructure, we could see the demise of classical cryptography before 2030.

Parting thoughts

The post-quantum timeline is dynamic and evolving, but it's still important that all businesses—especially those in the verticals mentioned earlier—begin taking stock of their machine identities and stay up to speed on developments in quantum computing.

Remember: now is not a time to panic. It's a time to look to the future, to see PQC in a more comprehensive way. To ensure you have the visibility, automation, and crypto-agility you need to not just survive in a world with quantum computers—but thrive.

Bolster your PQC readiness with the Venafi Control Plane

Learn how you can prepare your business for quantum computing threats with automated, **crypto-agile machine identity management.**

Venafi

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. To learn more, **visit venafi.com**