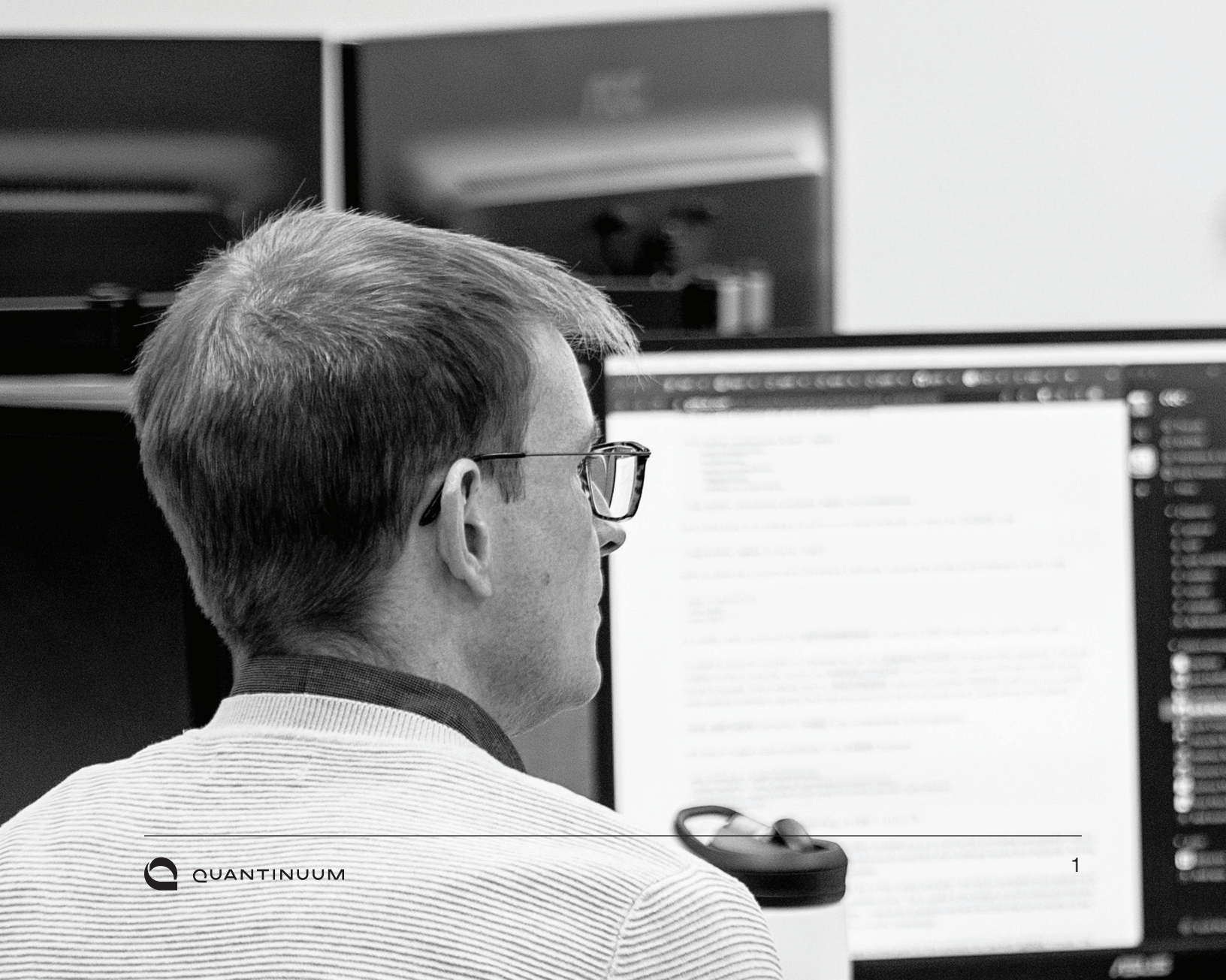
7 steps to build quantum resilience

QUANTUM ORIGIN

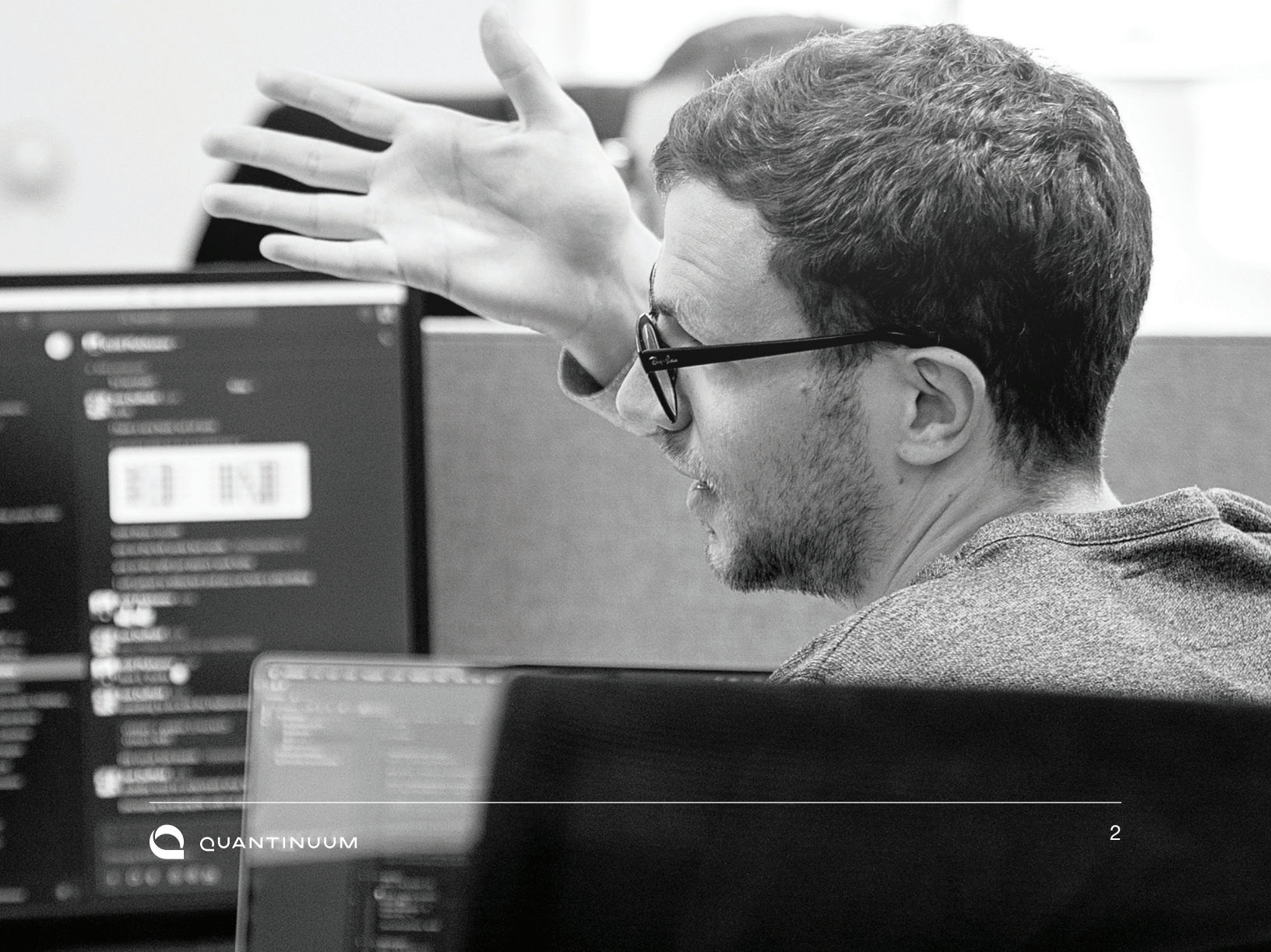
QUANTINUUM

To harness the potential of quantum computing,

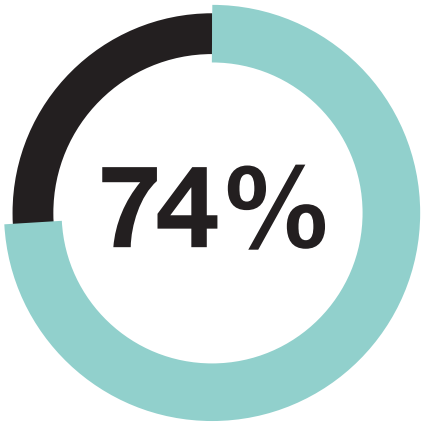
organizations need to act now



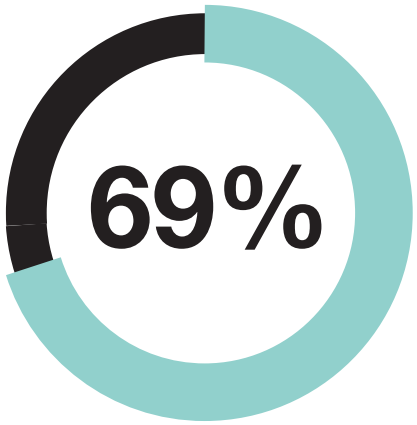
Quantum computing promises to be a transformative advancement within the enterprise tech arsenal. But as we've seen with previous new technologies, the development of such capabilities creates new risks and vulnerabilities, and quantum is no different. In fact, the threat quantum computing poses to the existing encryption methods on which most organizations rely, might be the biggest challenge security leaders will ever face. Given the prospects of such a challenge, enterprises need to start building the infrastructure, partnerships and skills to tackle this threat well ahead of time, or they will quickly find themselves at risk.



The accelerated rise of **quantum computing**



74% of recently surveyed respondents **agree that those who fail to adopt quantum computing solutions will fall behind**.*



69% of enterprises across the globe reveal they **have adopted or are planning to adopt quantum computing in the next year**.*

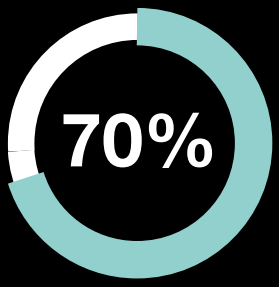
These results suggest that we are past the point of speculation on the value of quantum computing and that **it's no longer a matter of if quantum will provide an advantage, but when**. While this shift will bring immense value, it comes with significant risks.

*Zapata Enterprise and Quantum Adoption Survey, December 2021.

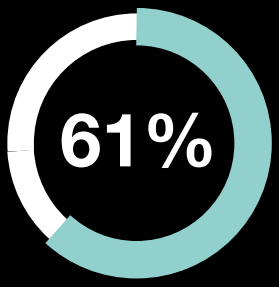
What about
quantum security?

Fault-tolerant quantum computers will be able to break some of today's widely used encryption standards, meaning that computer systems and **sensitive data that is not protected using quantum-safe measures will be at risk**. The longer the migration to quantum-safe standards is postponed, the more data remains at risk.

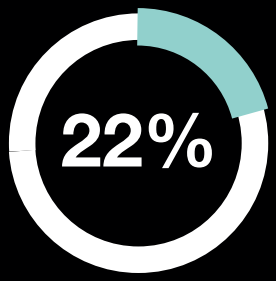
Many security professionals recognize this risk and the urgency of implementing measures to protect their sensitive data from this type of attack, but less than a quarter believe that they have appropriate security measures in place today.



70% of security professionals anticipate new technology will compromise current encryption techniques*



61% of security professionals expect current encryption to be compromised in the next two years*



22% of security professionals believe that they are prepared for a quantum attack today*

20+ billion

The World Economic Forum "estimates that **over 20 billion digital devices will need to be upgraded or replaced with quantum cryptography in the next 10-20 years**."**

*Quantum Computers Will Soon Be Able To Breakconventional Data Encryption: A Global Survey Of Security Professionals, Dimensional Research, 2021.
**https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf.

What leading technology decision makers can do **today**

The question remains, how to begin your quantum-resilience journey? Building this resilience is complex, and enterprises will need time to develop their quantum resilience strategy before they can deploy it. And although quantum algorithms are not yet ready for widespread use until the standardization process finishes in 2024, there is so much work to prepare for these changes.

To that end, **there are seven steps your organization can take today to assist you towards making your organization quantum resilient.**

7 steps to
quantum resilience

1. **Know your data assets**
2. **Identify uses of cryptography**
3. **Prioritize systems for migration**
4. **Speak to vendors**
5. **Test algorithms for home-grown software**
6. **Consider use of hybrid mode**
7. **Ensure crypto agility**

1 Know your data assets

Switching to quantum-safe algorithms cannot happen all at once. Even small businesses have far too many interlocking systems to expect to flip a switch and become secure. As a result, prioritization is critical. You need to identify the data that will pose the biggest organizational risk if it were to be breached. **You need to understand exactly what data you have, and how vulnerable it is to attack**. Data that is particularly sensitive, and vulnerable to the "hack now, decrypt later" attacks should be prioritized above less sensitive data that isn't transmitted freely.

2 Identify uses of cryptography

As well as identifying which data is important, technology leaders should catalog where quantum vulnerable algorithms are currently being used. For a variety of reasons, not all systems will be affected equally. Symmetric encryption, such as AES, is far less affected by the quantum threat, requiring only a doubling of key sizes to remain secure. By contrast, RSA will be broken completely. Technology leaders need a very clear picture of the vulnerabilities present in each of their systems.

3 Prioritize systems for migration

Once a clear view of sensitive data is established and the cryptographic protections have been determined, it's time to prioritize your migration. This requires a good old-fashioned risk management conversation, where you **use the collected data to identify the largest vulnerabilities to your organization from a potential quantum threat**.

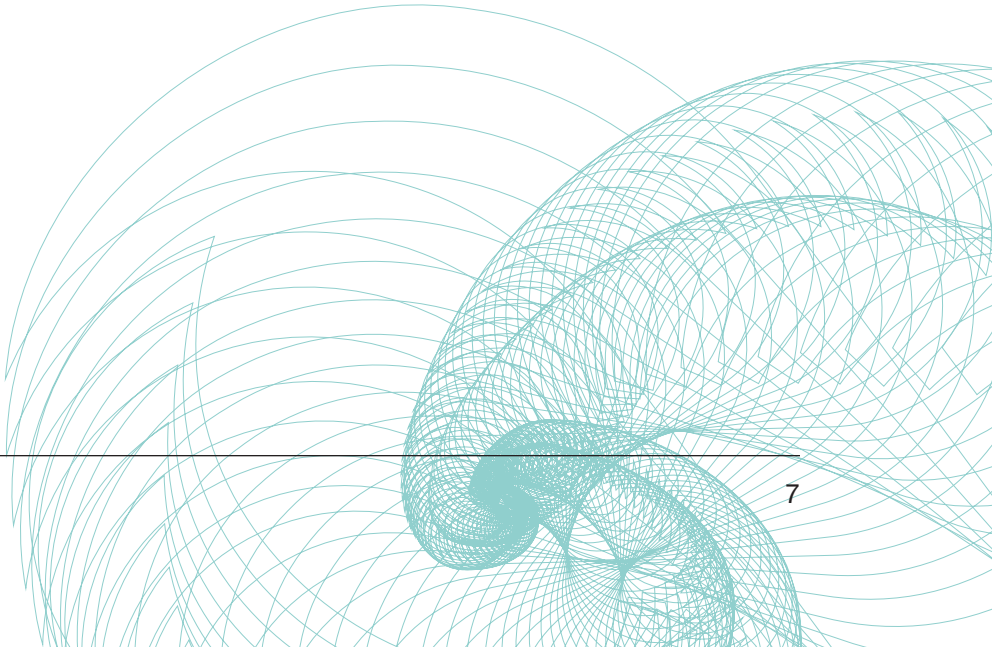
By far, the biggest concern should be the "hack now, decrypt later" concept, since this is a type of attack that may already have begun. This requires attention to encryption use cases, more than digital signatures. Mitigating this risk before it gets worse should be a top priority. Beyond this, the list will be driven by your own business imperatives, and your sense of what could be most damaging to your organization.

4 Speak to vendors

It's likely your IT infrastructure is a combination of home-grown software and third-party systems. In fact, for all but the largest of organizations, the amount of third-party software will dwarf the home-grown systems.

Now is the perfect time to be **asking your vendors about their plan for adopting quantum secure measures**. A good vendor should have a clear roadmap already in place and will have been testing the candidate algorithms in preparation for 2024. Some may even allow you to access builds of their software that already support the candidate algorithms, albeit in pre-standardization form. See the later section on hybrid modes to learn more about this.

If a vendor cannot answer this clearly, this might be a time to evaluate whether that vendor has a future with your organization. If nothing else, you should make it clear that a lack of a plan is unacceptable and set a clear date by which you expect to have a more detailed conversation. The same applies to contractors serving government organizations and meeting agency timelines and requirements.



5 Test algorithms for home-grown software

If your company develops its own software, then now is the time to **begin testing the NIST finalist algorithms to understand the impact they will have on performance and behavior of existing systems**.

The algorithms have different properties to the algorithms we use today. The only way to know how they will affect your systems is to implement them and experiment. A good place to start is with the Open Quantum Safe project, which provides many different implementations of quantum algorithms, designed for experimentation.

6 Consider use of hybrid mode

For companies concerned about the "hack now, decrypt later" attacks, **it may be possible to get the benefits of quantum security sooner, through the use of hybrid modes of operation**.

A hybrid mode of operation combines a traditional quantum-vulnerable algorithm, such as RSA, with a quantum-safe algorithm. This approach can be used in protocols such as TLS or SSH to strengthen security. To break into a hybrid mode system, an attacker would need to break the traditional algorithm as well as the quantum-safe algorithm. This means that using hybrid mode is no less secure than existing methods and may bring the benefit of being quantum-secure as well.

The downside of hybrid mode approaches is that they are not yet standardized. Until standardization is completed, they can only be deployed in closed-loop environments, in which both the sender and receiver agree on a non-standard approach to cryptography.

It's unclear whether hybrid modes will have a long-term future in quantum cryptography. In its quantum FAQs*, NIST acknowledges some applications may need the added security of hybrid mechanisms, even if it comes at the cost of performance. But for now, they represent an option for experimenting with non-standardized algorithms in some settings.

* https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs

7 Ensure crypto agility

Companies that prioritize long-term thinking are already looking at this. Ensuring crypto agility has two obvious benefits.

First, if a problem is found with one of the NIST finalist algorithms, or it turns out that a different option is better for a particular environment, then **swapping them out should be relatively easy**. It is inevitable that the most popular choice of quantum algorithm implemented worldwide will not be the best choice for every use case, as is reflected in NIST's decision to provide options.

Secondly, the continued use of deprecated cryptography is one of the main cryptographic security issues with deployed systems. For example, the cryptographic hash function SHA-1 has not been considered cryptographically secure since 2005. However, even though the SHA-2 family of hash functions have been recommended since 2002, it took NIST until 2015 before recommending that federal agencies stop using SHA-1 in digital signatures.

What is **crypto agility?**

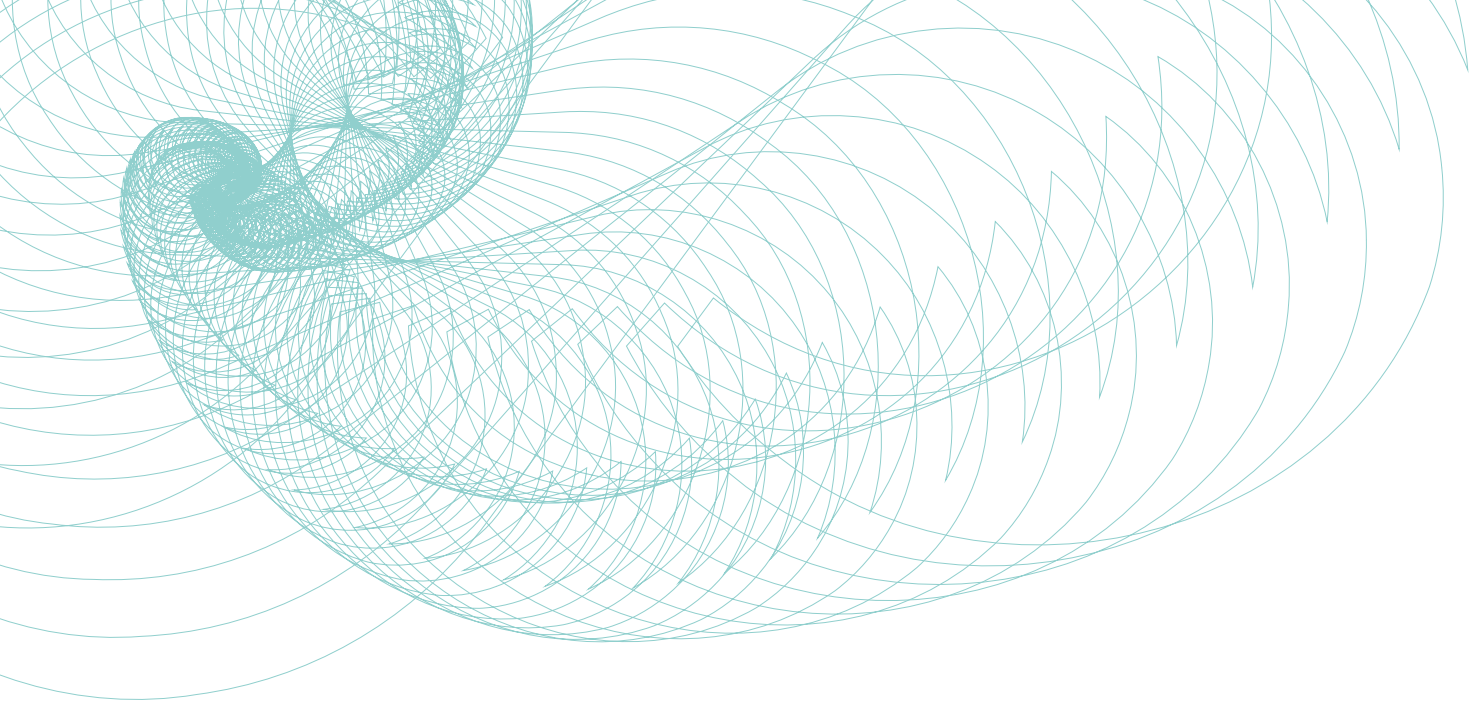
There is always the possibility that vulnerabilities will be discovered in newer cryptographic algorithms. It is therefore worth using the occasion of transitioning to quantum-safe measures to build-in crypto agility, by design. **Crypto agility is about how easy it is to transition systems and processes from one algorithm (or choice of parameters) to another**.

Why partner with **Quantinuum?**

At Quantinuum, we are home to some of the best quantum computing experts in the world. Our world-class scientists and engineers are on the leading edge of their fields and are accelerating cybersecurity to help clients build quantum resilience.

Our cybersecurity solution, Quantum Origin, provides quantum-computing-hardened cryptographic keys, making them the strongest on the planet. It helps customers develop a secure and crypto-agile environment as it supports traditional algorithms, such as RSA and AES, as well as quantum cryptography algorithms currently being standardized by the National Institute for Standards and Technology (NIST).

Quantum Origin is simple to deploy and integrates with leading key management technologies providing you with a straightforward path to future-proof data protection.



It is worth remembering that while quantum computing poses a threat to cybersecurity, it also offers new techniques for strengthening existing systems.

You need to embrace these developments now to build future resilience, because delaying preparations for the quantum threat could be a costly decision for your organization.

Would you like to talk to an expert about how you can use the extraordinary power of quantum computing to build resilience?

Contact us at origin@quantinuum.com

Learn more about
QUANTUM ORIGIN

QUANTINUUM