SENETAS

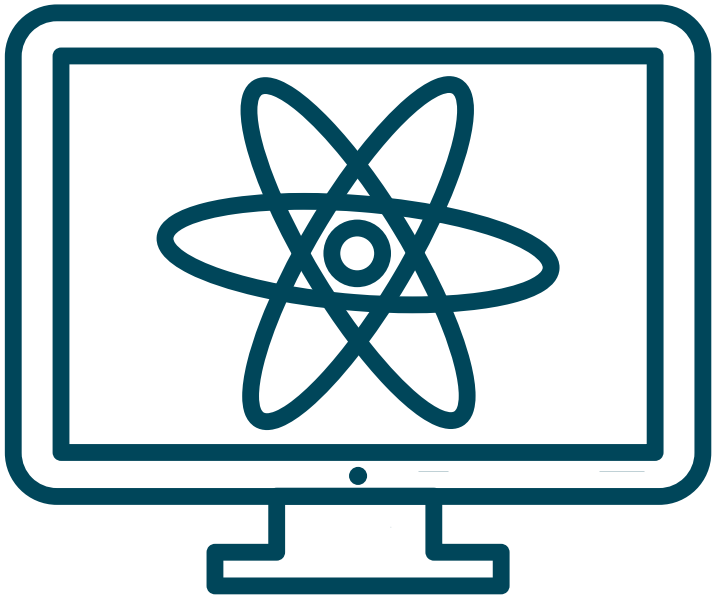
Security without compromise

WHY TOMORROW'S **QUANTUM TECHNOLOGIES** THREATEN TODAY'S **ENCRYPTION SECURITY**

A REVIEW OF THE QUANTUM THREAT

WHAT IS A QUANTUM COMPUTER?

A new type of computer that seeks to exploit the properties of quantum mechanics, such as entanglement and superposition, to exponentially speed up computing performance for some mathematically hard problems.



QUANTUM BITS – THE BUILDING BLOCKS OF A QUANTUM COMPUTER

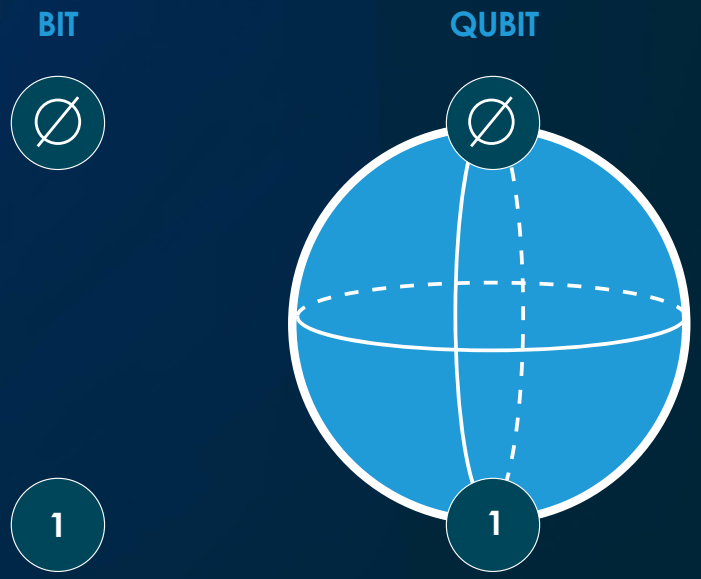
The keys to understanding the power of a quantum computer are superposition and entanglement.

- Classical bit: 0 or 1
- Quantum bit (qubit): Superposition of 0 and 1

'N' Entangled qubits represents all 2N states simultaneously. Entangled qubits are connected in such a way that when we measure them, their state is mathematically related.

Every additional qubit leads to an exponential increase in the number of states that can be represented. EG two qubits = 4, three qubits = 8 etc.

WOW! With just 300 qubits it is possible to represent more state simultaneously than there are atoms in the observable universe!

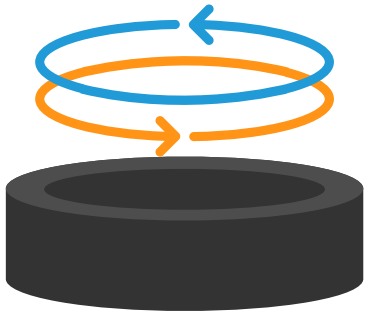


QUANTUM BITS – THE BUILDING BLOCKS OF A QUANTUM COMPUTER

Qubits can exist in many physical forms…

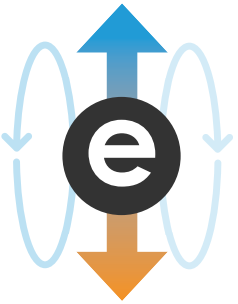
However, they are very fragile. Think of them as soap bubbles – they tend to have unwanted interactions with their environment which leads to their collapse (decoherence).

For reliability, we need multiple copies of Qubits (error correction). Current estimates suggest we need 1000 physical qubits for every logical qubit, which means we need around 1million physical qubits to perform reliable calculations.

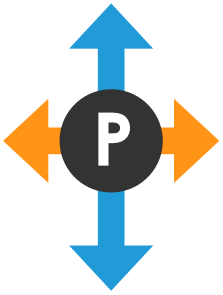


Persistent current in a superconducting circuit

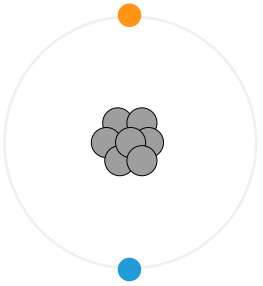
QUBIT



Electric Magnetic Field

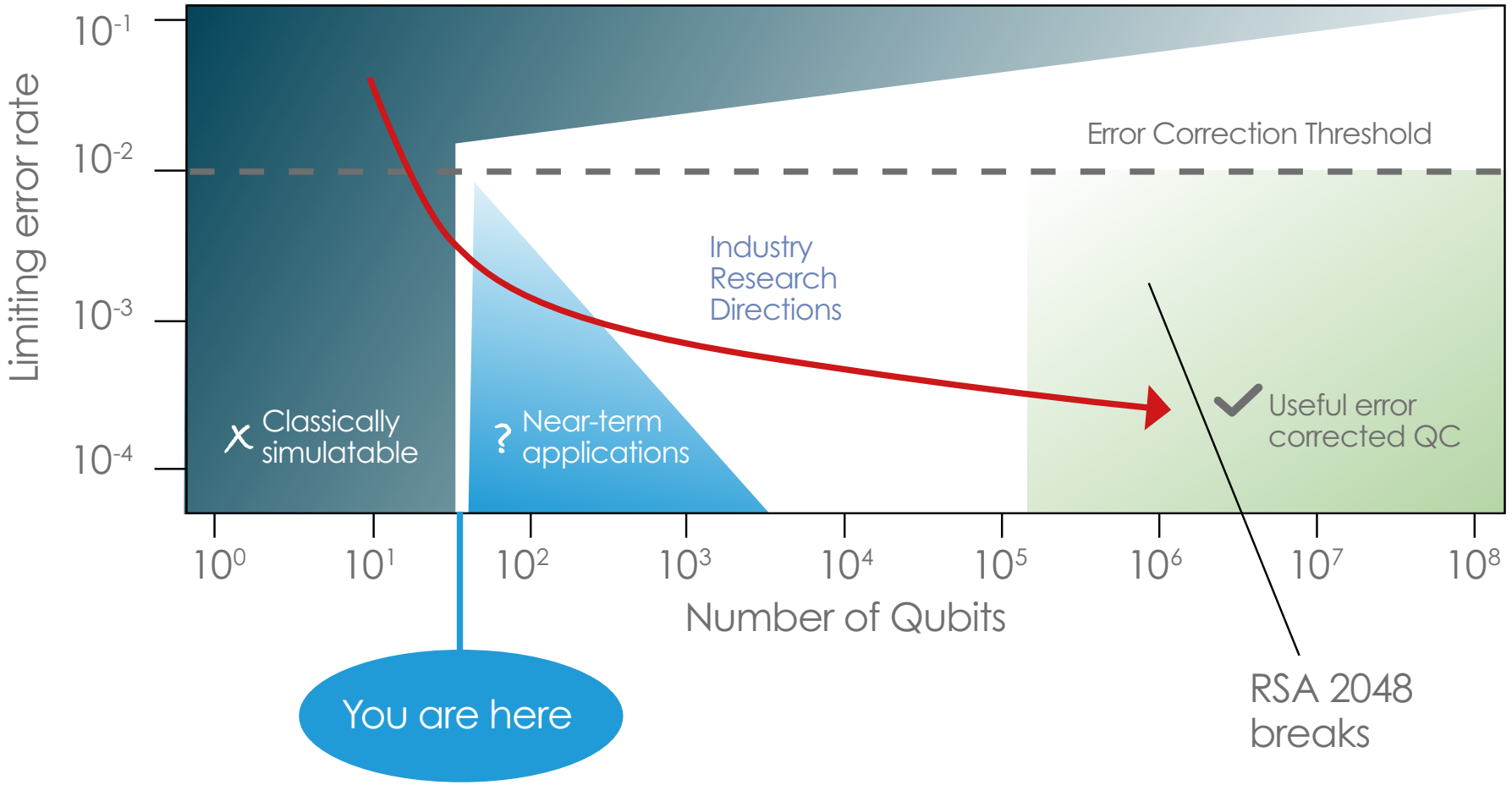


Photon polarization



Atom Internal State

QUANTUM BITS – THE BUILDING BLOCKS OF A QUANTUM COMPUTER



QUANTUM BITS – THE BUILDING BLOCKS OF A QUANTUM COMPUTER

Grover 1	Cryptographic algorithm	Type	Purpose	Impact from large scale QC
	AES	Symmetric key	Encryption	Longer keys needed
	SHA-2, SHA-3	----------	Hash functions	Larger output needed

Shor 2	Cryptographic algorithm	Type	Purpose	Impact from large scale QC
	RSA	Public key	Signatures, Key establishment	No longer secure
	Digital Signature Algorithm	Public key	Signatures, Key establishment	No longer secure
	ECDSA (Elliptic Curve DSA)	Public key	Signatures, Key establishment	No longer secure

QUANTUM DEFENSES

#1 Quantum safe cryptography

Our best defence against quantum computers is likely to come in the form of Quantum Resistant Algorithms

- Quantum Signature schemes: Dilithium, Falcon, Rainbow
- Key Encapsulation Mechanisms: SABRE, NTRU, Kyber, McEliece

However, performance in real-world protocols varies due to key size, padding schemes and latency.

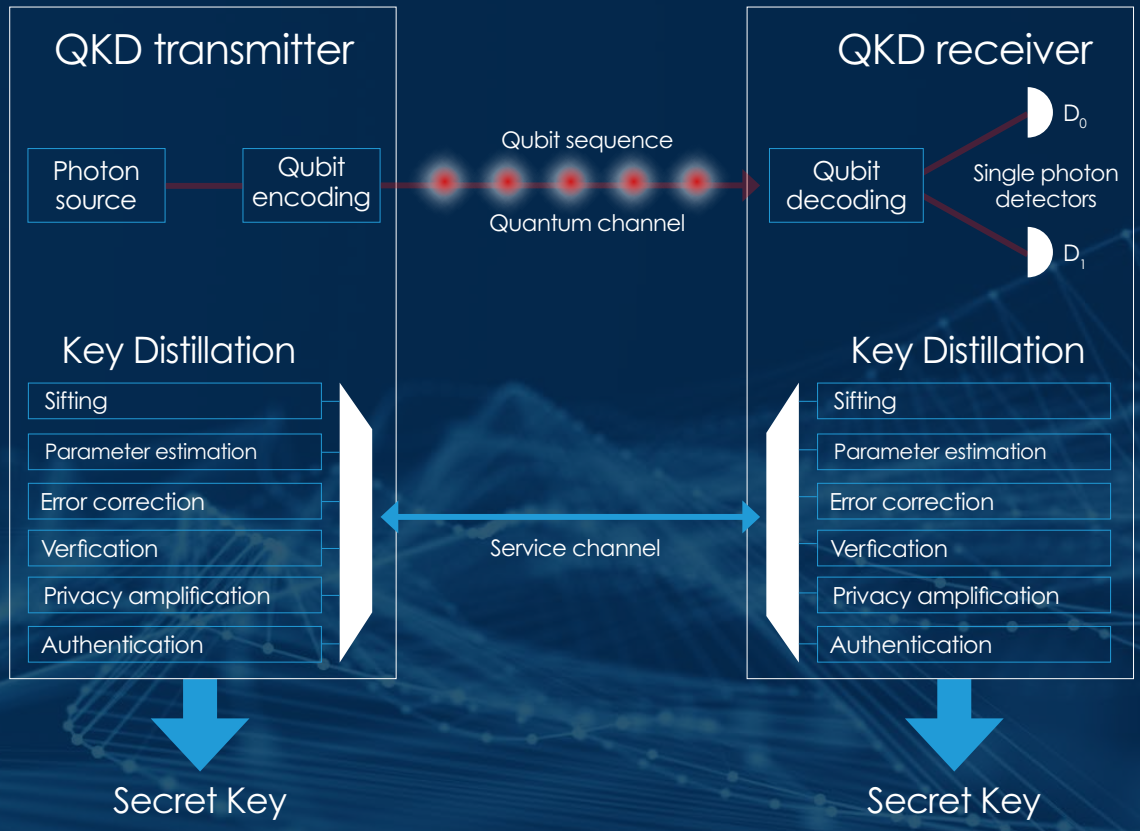
The first NIST draft QRA standards are expected in 2022. These will specify new algorithms for:

- Digital signatures
- Public key encryption
- Key encapsulation mechanisms

QUANTUM DEFENSES

#2 Quantum key distribution

- Harnesses the properties of quantum mechanics to allow secrets to be shared between two parties
- QKD is a fundamentally different approach to key sharing. Its security relies on the principle that observation cause perturbation – IE the act of eavesdropping or interception changes the quantum state.
- QKD doesn't prevent eavesdropping, but it guarantees detection.
- Commercial QKD systems are already in use, helping to secure next-gen communications networks around the world.



THE NEED FOR QUANTUM RESILIENCE

"The ability of a digital ecosystem to remain secure against a future quantum computing attack."

THREE REASONS TO CONSIDER QUANTUM RESILIENCE URGENT

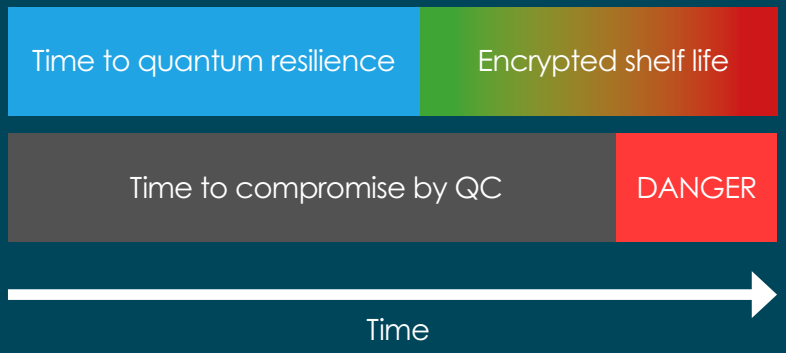
01 Your data has an expiration date

YOUR DATA HAS AN EXPIRATION DATE

Encrypted data today is Quantum Vulnerable, it has no defence against future quantum threats

Sensitive data often has a long shelf life, with some data types remaining relevant for decades, or more.

Long term Quantum Vulnerable data is already decaying, with the risk of exposure increasing over time.
It is also susceptible to "harvest now, decrypt later" threats.



Expiration date

Hours - temporaty credentials

Months - corporate earnings

Years - banking information, credit cards

Decades - trade secrets, classified information

Lifetime - DNA data, personal information

THREE REASONS TO CONSIDER QUANTUM RESILIENCE URGENT

02 This is an Internet scale problem

IMPACT OF A PRACTICAL EXPLOITATION OF SHOR'S ALGORITHM

CRYPTO CURRENCIES

EMAIL

SOFTWARE UPDATES

WEBSITES

MOBILE APPS

ELECTRONIC PAYMENTS

DATA PRIVACY

THREE REASONS TO CONSIDER QUANTUM RESILIENCE URGENT

03 The transition is going to be harder than you think

MOST CRYPTOGRAPHIC ASSETS ARE HIDDEN

Most organisations have a problem when it comes to identifying where their cryptographic keys are being stored or used, across…

- Applications
- Browsers
- Platforms
- Files
- Modules

This lack of visibility creates significant risk.

PRACTICAL STRATEGIES TO PROTECT YOUR ORGANISATION TODAY

OPTIMISTIC SCENARIO: ACCELERATED PATH TO QUANTUM RESILIENCE

The optimistic scenario assumes rapid migration to a Quantum Safe Infrastructure.

+ limited progress in Quantum Computing development.

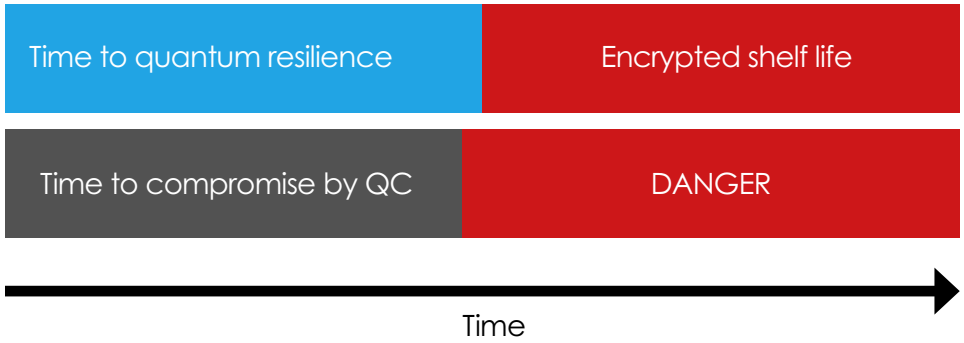
Assuming the introduction of truly secure, quantum resistant algorithms, the exposure window disappears and there is no loss of security.

PESSIMISTIC SCENARIO: QUANTUM COMPUTING BREAKTHROUGH

The pessimistic view (from a security perspective) assumes a breakthrough in the Million Qubit roadmap.

+ delays in the implementation of a Quantum Safe Infrastructure.

The result would be a complete loss of security for all current Public Key encryption before we have a chance to prepare.

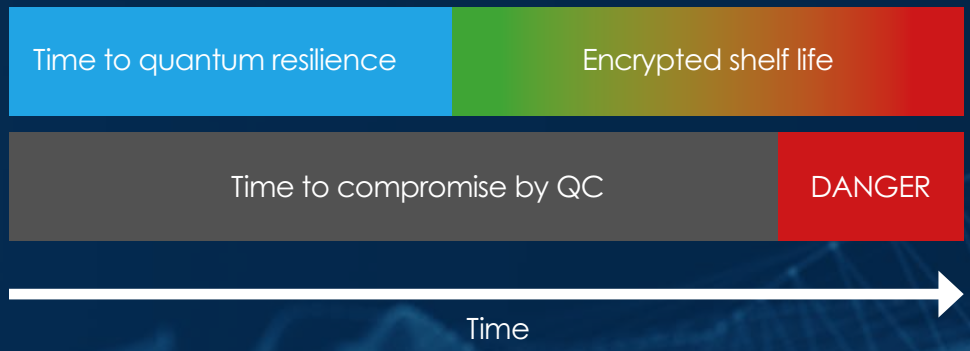


REALISTIC SCENARIO

Achieving quantum resilience will take some time, but that doesn't mean we have to wait before we act.

We can begin to deploy hybrid encryption now and combine today's quantum vulnerable PKI with tomorrow's quantum safe PKI.

Assuming quantum resistant algorithms prove effective we can reduce, or possibly remove the window of vulnerability.

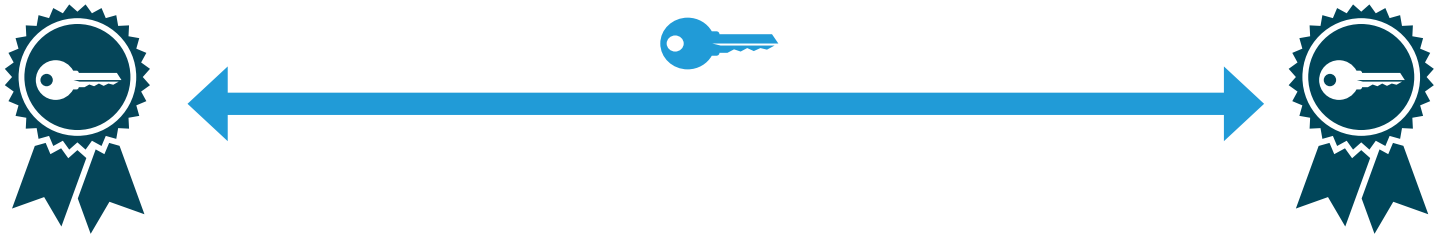


QUANTUM SAFE, HYBRID KEY ESTABLISHMENT

In the short term the new quantum algorithms can be used in a hybrid mode in conjunction with today's algorithms to provide an additional layer of defence even before they are standardised.

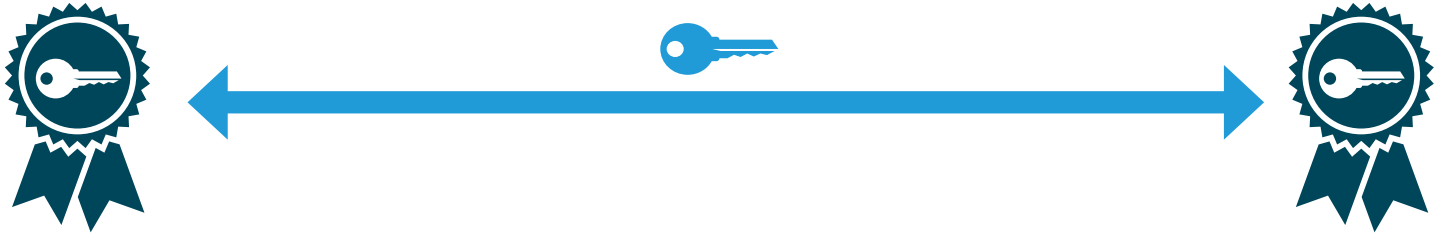
Perform classic authentication and key establishment

Eg RSA, ECC etc

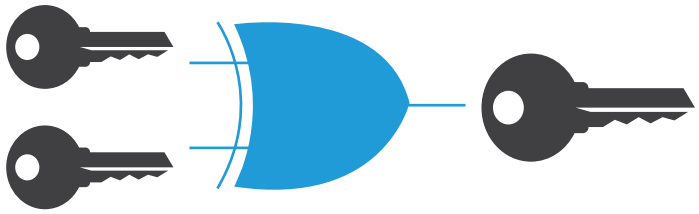


Perform additional quantum safe authentication and key establishment

E.g. Falcon, Saber



Combine keys



PATH TO QUANTUM RESILIENCE

DISCOVER

Conduct inventory to identify quantum vulnerable assets.

CLASSIFY

Categorise with respect to criticality, disclosure sensitivity AND on shelf life / data lifecycle.

PRIORITISE

Use a risk methodology to prioritise the most important components.

ENGAGE

Work with internal and external experts to implement emerging quantum resistant algorithms.

CRITICAL AREAS OF FOCUS

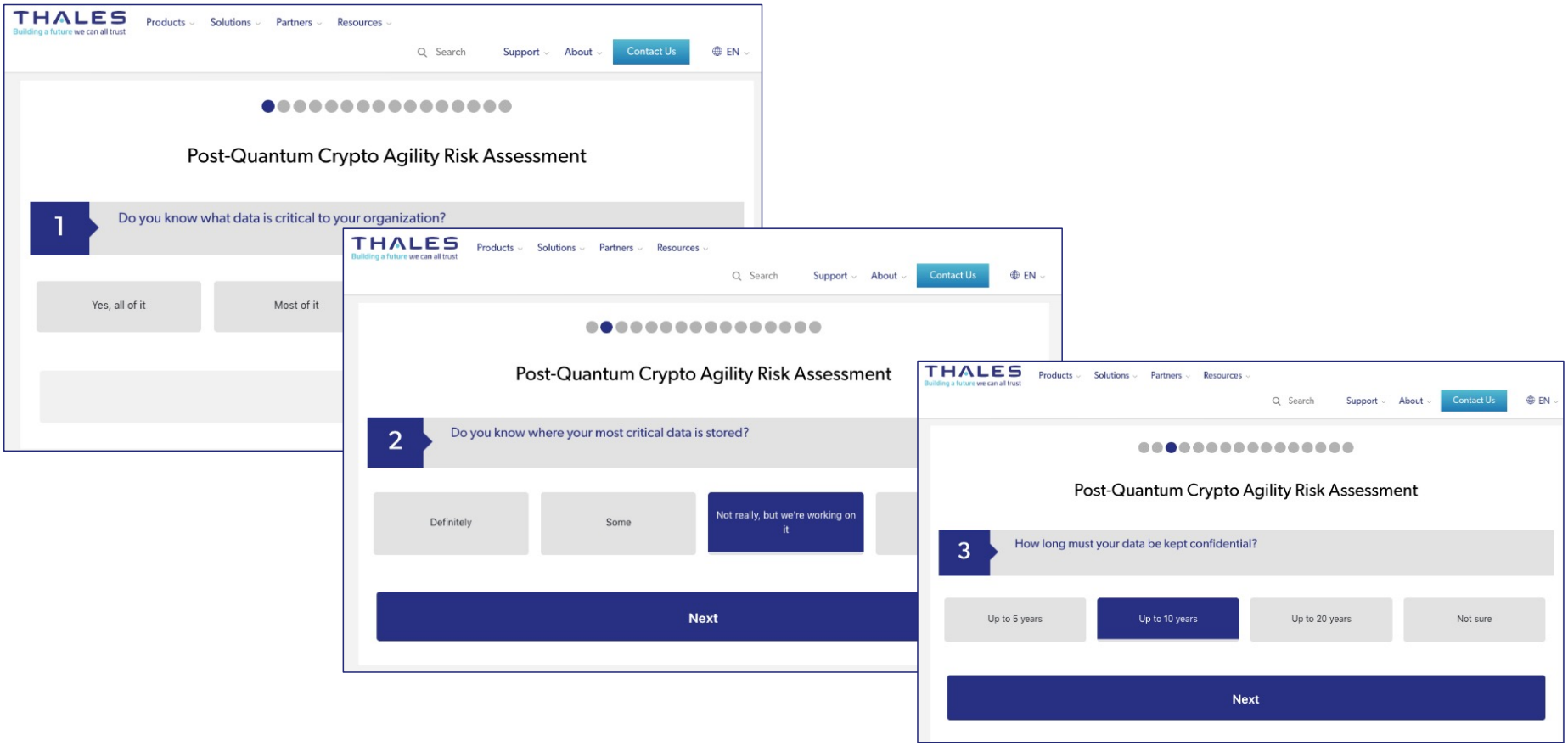
Data-in-Motion

- **Long term data often moved between data centers**
  - 100Gbps (or more) at risk!
- **Data in motion is often harvested**
  - Syphoned from lines and held for future use
- **By the time you know it's too late!**
  - Data in motion breaches are under-reported

Key Management

- **Keys vulnerable to loss, theft or corruption**
  - OS & Application vulnerabilities put keys at risk
  - Subject to virtual & cloud cloning attacks
- **Keys & data stored together**
  - If you can access the encrypted data, you can access the key
- **No assurance of keys**
  - Varied access methods create security & access issues

POST-QUANTUM CRYPTO AGILITY RISK ASSESSMENT TOOL



https://cpl.thalesgroup.com/encryption/post-quantum-crypto-agility-tool

KEY TAKEAWAYS

Quantum is coming	Know your risks	Approximate Physical Qubits	Start Today
• Quantum capabilities are accelerating • NIST is finalizing quantum safe standards • PKI based crypto will become obsolete	• Long term data is at risk, if using classic technologies • Consider that it is vulnerable to harvesting and early attacks	• Crypto Agility is the best practice; requires supporting infrastructure • Take a hybrid approach by using classic & quantum-safe crypto solutions	• Assess your crypto agility maturity and readiness • Design a quantum safe architecture • Be ready for change, even after standards are established

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales and within government & defence sectors by Thales Defense & Security Inc.

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its SafeNet brand.

THALES

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers; including:

AUCLOUD Data#3 DATACOM dimension data

DXC IBM macquarie GOVERNMENT VOCUS communications

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 35 countries.

From certified high-assurance hardware and virtualised encryption, to secure file sharing with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61 (03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** info@senetas-europe.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has an encryption solution to suit. Our certified high-assurance encryptors protect data across networks operating at speeds from modest 10Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 5Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

SECURE FILE SHARING

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Disarmer extension.

DISARM MALICIOUS CONTENT

Votiro Disarmer leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.