Microsoft Security

Microsoft Quantum Safe Program Strategy Overview

Kevin Reifsteck, Director for Cybersecurity Policy

Kevin Reifsteck

Director for Cybersecurity Policy

Kevin focuses on quantum safety and critical infrastructure protection issues. Prior to joining Microsoft, he served in roles as a Director for Critical Infrastructure Cybersecurity for the National Security Council (NSC) and as an analyst for the Central Intelligence Agency (CIA).

Terminology

Quantum ready

Term used for discussion of *developing and implementing* quantum computing capabilities

Quantum computer

Using quantum mechanics, computational units are known as Qubits

Quantum safe

Term used for the discussion of *security topics* including *quantum safe cryptography*

Post quantum cryptography

Quantum resistant algorithms applying mathematical challenges to reduce the risk of quantum computing capabilities

Quantum computing
is a game changer
for humanity

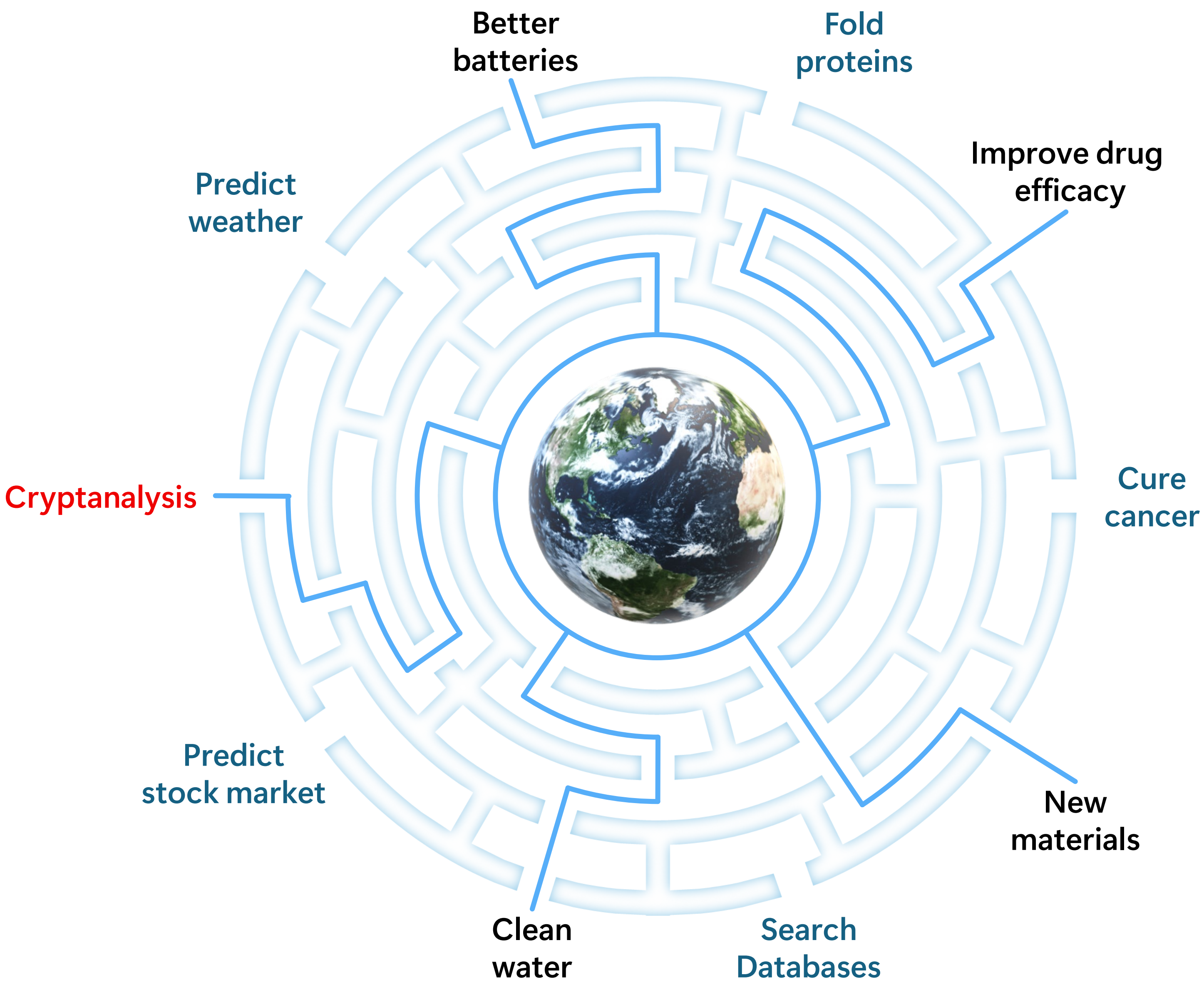
Shifts in technology capabilities bring new challenges and opportunities

1980s	1990s	2000s	2010s	2020s	2030s
Desktop Computing	The World Wide Web	Mobile Computing	Cloud Computing	Generative AI	Quantum Computing
Not pen and paper	Not my network	Not in my control	Not my servers	Not my content	Not 1’s and 0’s

Microsoft quantum vision

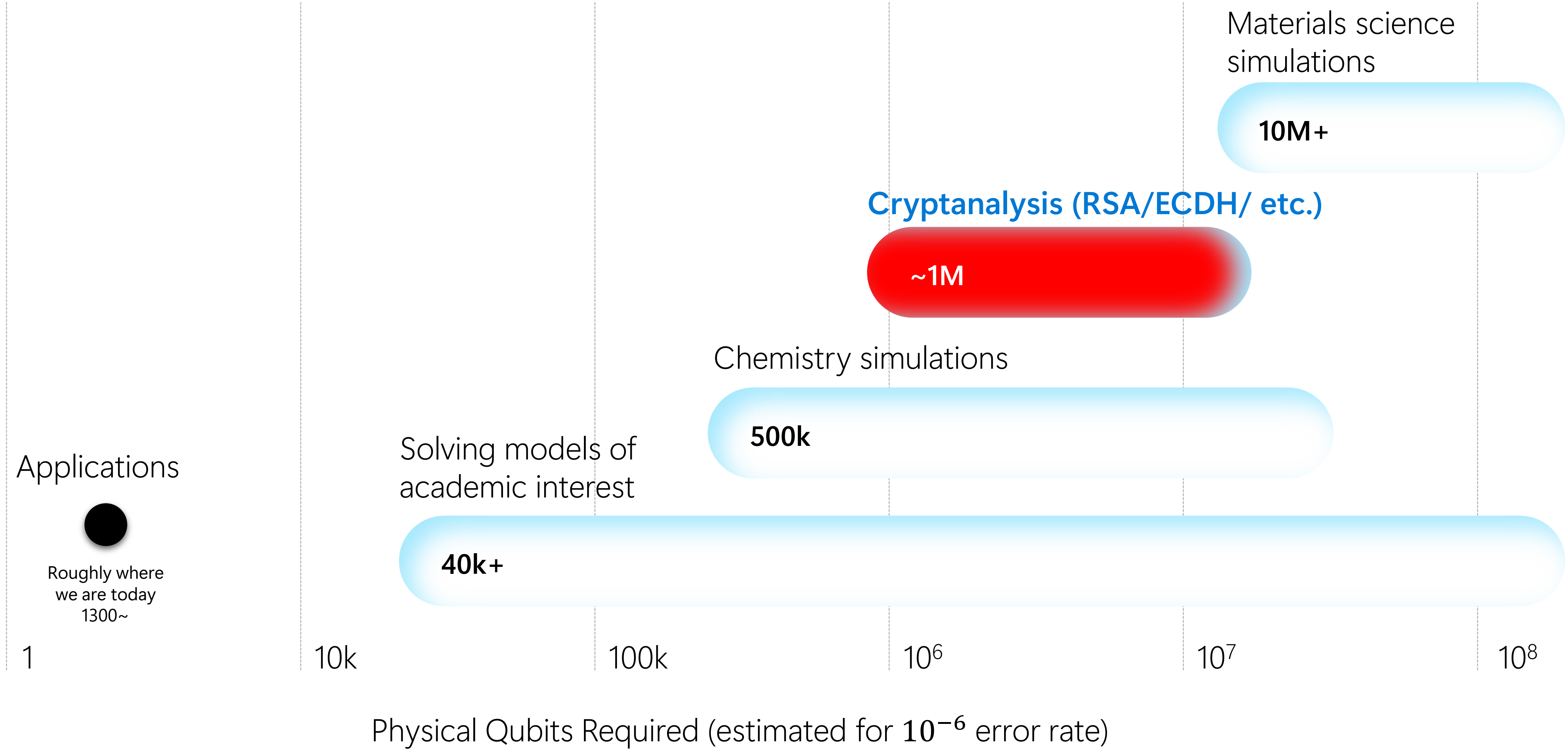
- Delivering the **first reliable quantum machine** with Atom Computing, integrated with **AI and supercomputing** in the cloud.
- Building a **hybrid cloud platform** that combines quantum, HPC, and AI to solve complex challenges.
- Enabling **secure by design applications** through scalable, hybrid compute power.

Quantum computers will excel at solving specific problems



Modern Cryptography - Understanding the hype vs. reality

Today's quantum computers do not pose a legitimate threat to cryptographic systems
Practical quantum advantage begins with millions of qubits



The sooner organizations start their quantum-safe transformation, the safer they will be.

Systems are vulnerable already today

1. Encrypted data can be recorded and stored today to be decrypted in the future (harvest now, decrypt later)
2. Hard-to-update systems with long deployment lifetimes

Multi-year and complex transition

1. The scale of reaching quantum-safety is pervasive, spanning multiple security layers.
2. Inventorying and updating all asymmetric cryptography usage is a complex and expensive process

Microsoft Quantum Safe Program (QSP)

The QSP is a comprehensive and company-wide effort to enable Microsoft, our customers, and partners, to transition smoothly and securely into the quantum era.

The program is governed by the QSP leadership team with representatives across all major business groups, research and engineering divisions, and functions.

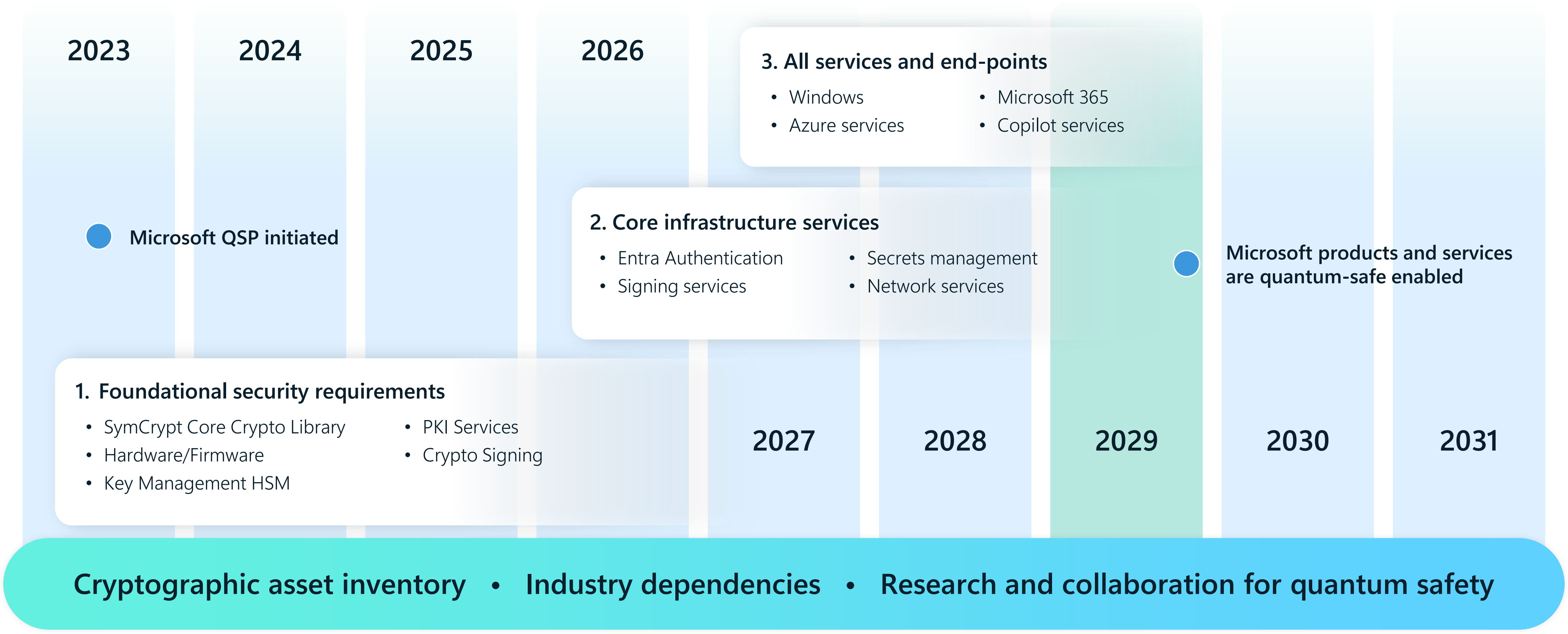
Aka.ms/QSP/Strategy-2025

QSP Priorities

1. Make Microsoft quantum safe by updating Microsoft first- and third-party services, supply chain, and ecosystem to become quantum safe and crypto-agile
2. Support customers, partners, and ecosystems to become quantum safe with appropriate tools and guidance
3. Promote global research, standards, and solutions for quantum-safe technologies and crypto-agility

Quantum Safe Timeline

Microsoft QSP strategy and timeline



Your first step - crypto inventory

Prioritize the risk based on what you already know

1. Follow your business continuity programs (incident response, disaster recovery), focusing on cryptographic weaknesses within critical business units and environments first.
2. Spot the most vulnerable areas for harvest-now, decrypt-later (HNDL), such as sensitive communications, critical storage devices, financial transactions, and business processes.
3. Group cryptographical assets based on how they protect information in transit, at runtime, or at rest.
4. Implement a **shift-left** approach: resolve issues in design and code where possible.

Discover **storage** assets

Identify and organize certificates and keys held by KMS and HSM for secure management and auditing.

Safeguard **network** channels

Protect critical internal and external network channels to prevent unauthorized access to cryptographic assets.

Upgrade **code** early

Implement cryptographic upgrades at the start of the development cycle to improve security and efficiency.

Distinguish **runtime** encryption

Track encryption that is actively used versus dormant to maintain effective security controls.

Call to action

Modernize legacy systems

Retire, isolate, or migrate outdated systems to minimize vulnerabilities and enhance overall security posture.

Transition to cloud with PQC

Move critical services to cloud platforms supporting PQC-ready alternatives and upgrade symmetric key sizes to AES-256 wherever you can for increased protection.

Adopt PQC algorithms

Inventory your current cryptographic risk. Implement post-quantum cryptography algorithms, prepare for refactoring costs, and rotate asymmetric keys frequently to reduce exposure.

Government Policy Recommendations

01

Establish national cybersecurity priority

02

Align requirements and roadmaps

03

Adopt international standards

04

Set early and progressive timelines

05

Lead by example

06

Raise awareness

Aka.ms/QSP/Policy-2025

Microsoft Security