The journey to quantum safety

Practical path to resiliency against the quantum threat

Marc Stöcklin
Head of Security Research
IBM Research Europe - Zurich

Manuel Schindler
Openshift / DevX
Specialist Solution Architect

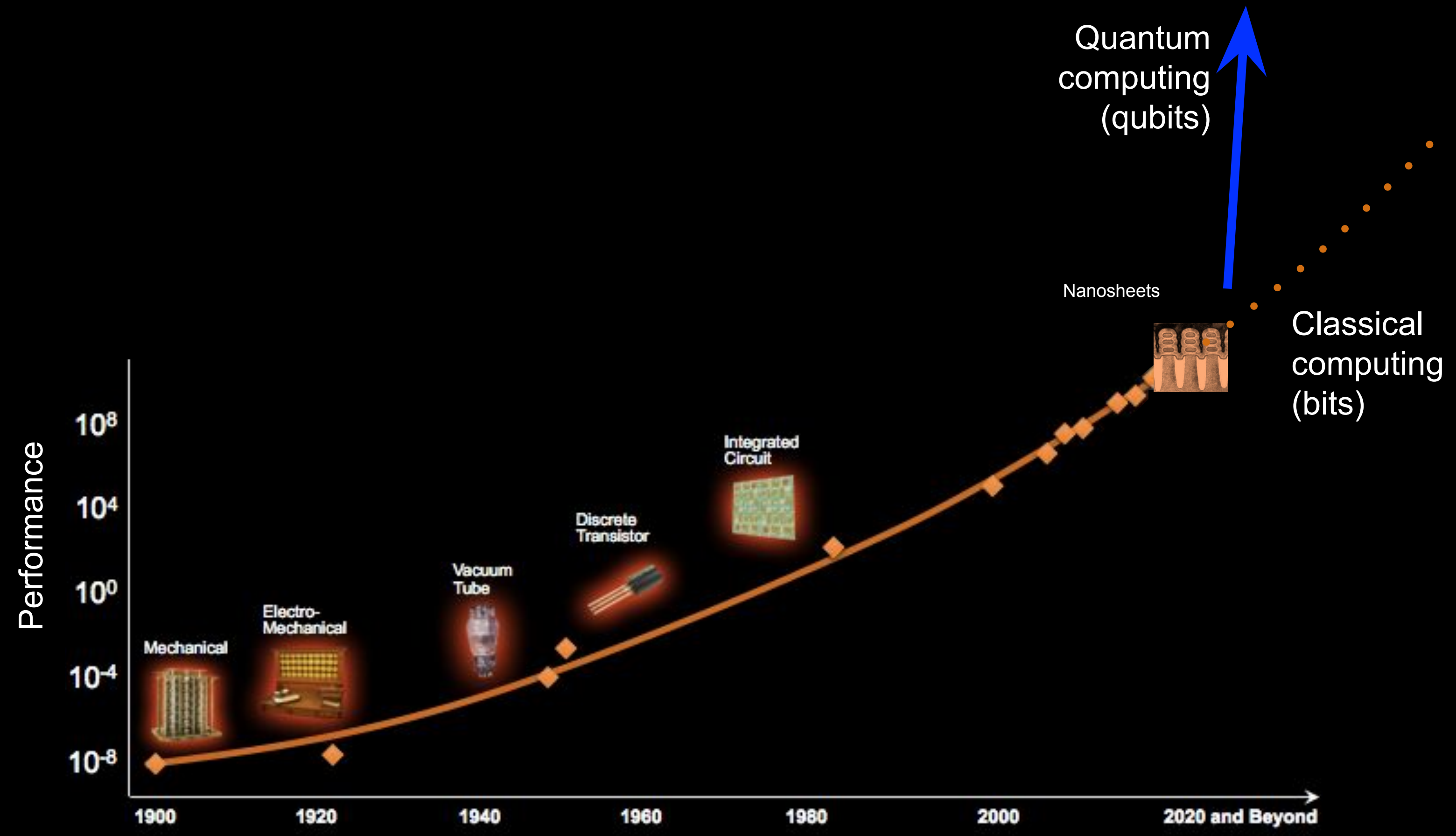
Agenda

- Quantum Computing
- Quantum Safe Cryptography
- Red Hat Strategy
- Migration to Quantum Safe

QUANTUM

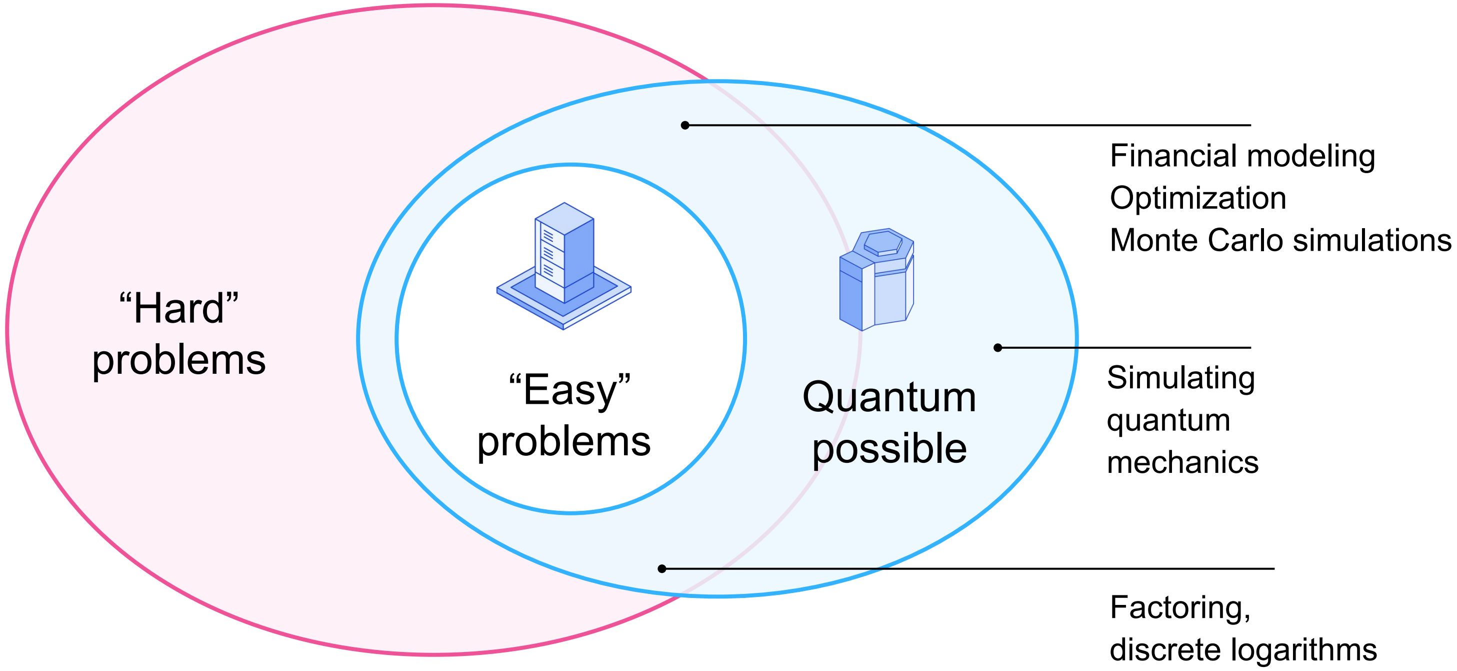
Beyond classical:

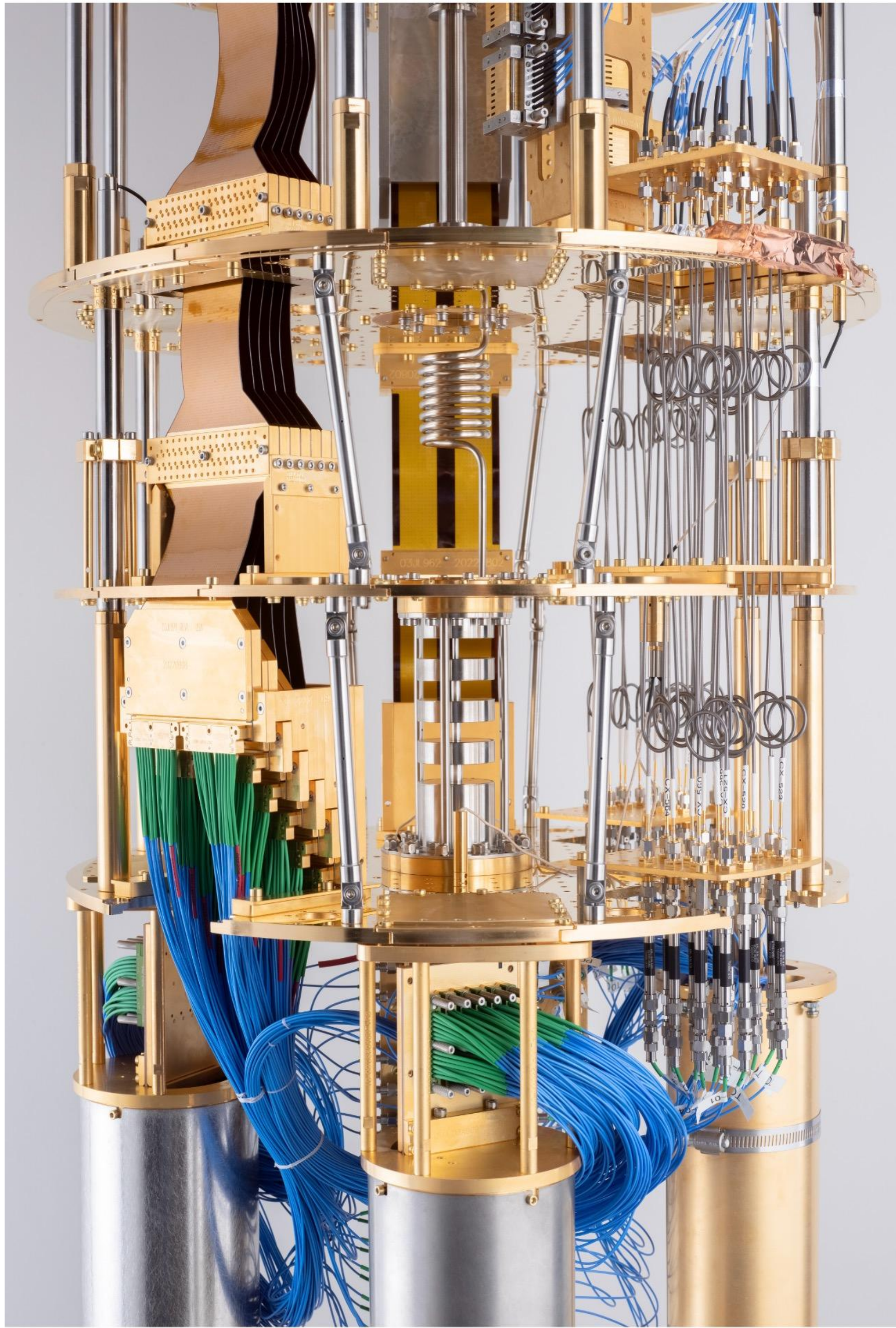
First time in history computing has branched



Why quantum?

Despite how sophisticated digital “classical” computing has become, there are many scientific and business problems for which we’ve barely scratched the surface.





Our modern world depends on cryptography

It is the ultimate line of defense.

Public key encryption • Digital signatures • Key exchange algorithms

RSA • DSA • ECC • ECDSA • DH

2048-bit integer number

2519590847565789349402718324004839857142928212620403202777
7137836043662020707595556264018525880784406918290641249515
0821892985591491761845028084891200728449926873928072877767
3597141834727026189637501497182469116507761337985909570009
7330459748808428401797429100642458691817195118746121515172
6546322822168699875491824224336372590851418654620435767984
2338718477444792073993423658482382428119816381501067481045
1660377306056201619676256133844143603833904414952634432190
1146575444541784240209246165157233507787077498171257724679
6292638635637328991215483143816789988504044536402352738195
1378636564391212010397122822120720357

Find prime factors

$$= p \cdot q$$

Expected computation time

The most powerful computer today:

Millions of years

Shor’s quantum algorithm:

Hours

The Post-quantum Cryptographic Transition

The migration will be a journey, not a flip of a switch. Red Hat anticipates a long, hybrid transition period to ensure stability and security before industry moves purely to PQC.

Classical (Yesterday)

Traditional cryptography has no quantum resistance.

PQ Capable (Today)

Hybrid PQC is now available for configuration to use, it is not on by default in RHEL 10.

PQ Ready (Tomorrow)

Hybrid PQC is enabled by default, with classical as configurable to use.

Deprecation/Removal (Future)

Classical algorithms will become deprecated and removed, hardening systems against downgrade attacks.

What can a cybercriminal do?

Before

Harvest confidential data to decrypt later

“Harvest now, decrypt later”

Urgency*

* for some data and systems

Availability of “cryptographically relevant” quantum computers

After

Decrypt lost or harvested confidential data by breaking encryption

Confidentiality

Disrupt business with manipulation through fraudulent authentication

Integrity

Manipulate digitally signed contracts and legal history by forging digital signatures

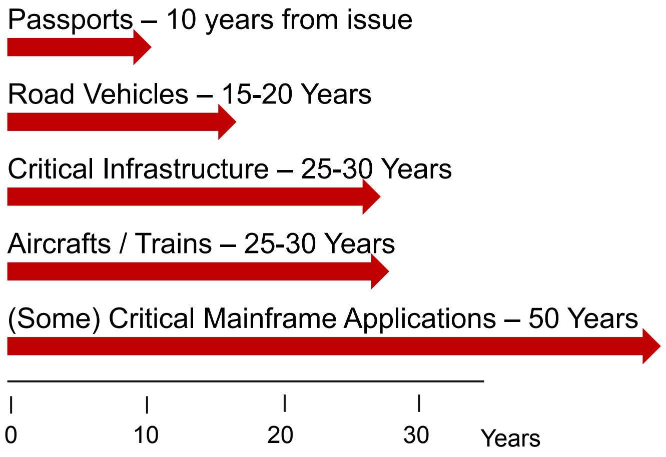
Authenticity

Cryptography is everywhere

and is used in trillions of transactions on billions of devices every day.

- Internet
- Digital signatures
- Critical infrastructure
- Financial systems
- Blockchain
- Enterprise

Systems have long update cycles



Passports – 10 years from issue

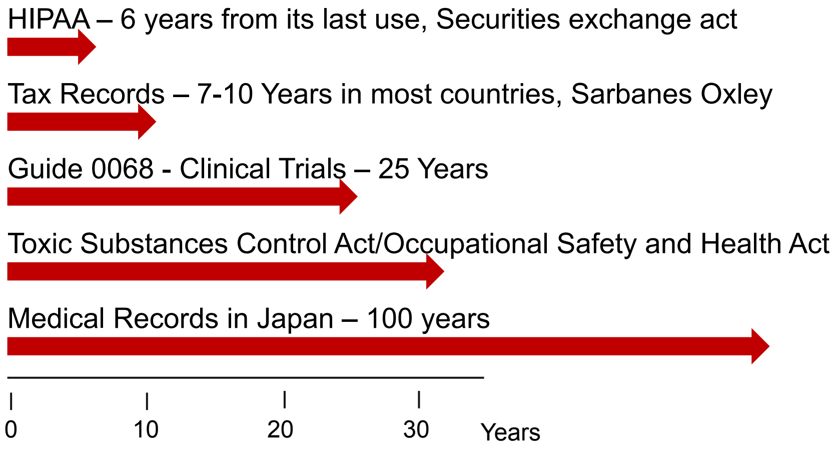
Road Vehicles – 15-20 Years

Critical Infrastructure – 25-30 Years

Aircrafts / Trains – 25-30 Years

(Some) Critical Mainframe Applications – 50 Years

Data must stay secure for long time



HIPAA – 6 years from its last use, Securities exchange act

Tax Records – 7-10 Years in most countries, Sarbanes Oxley

Guide 0068 - Clinical Trials – 25 Years

Toxic Substances Control Act/Occupational Safety and Health Act

Medical Records in Japan – 100 years

Quantum Safe Cryptography

2016

NIST PQC competition

Over 70 submissions of new cryptographic algorithms

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

2022

NIST algorithms selected

→ CRYSTALS-Kyber

→ CRYSTALS-Dilithium
→ Falcon
→ SPHINCS^{+}

2024

NIST standards released

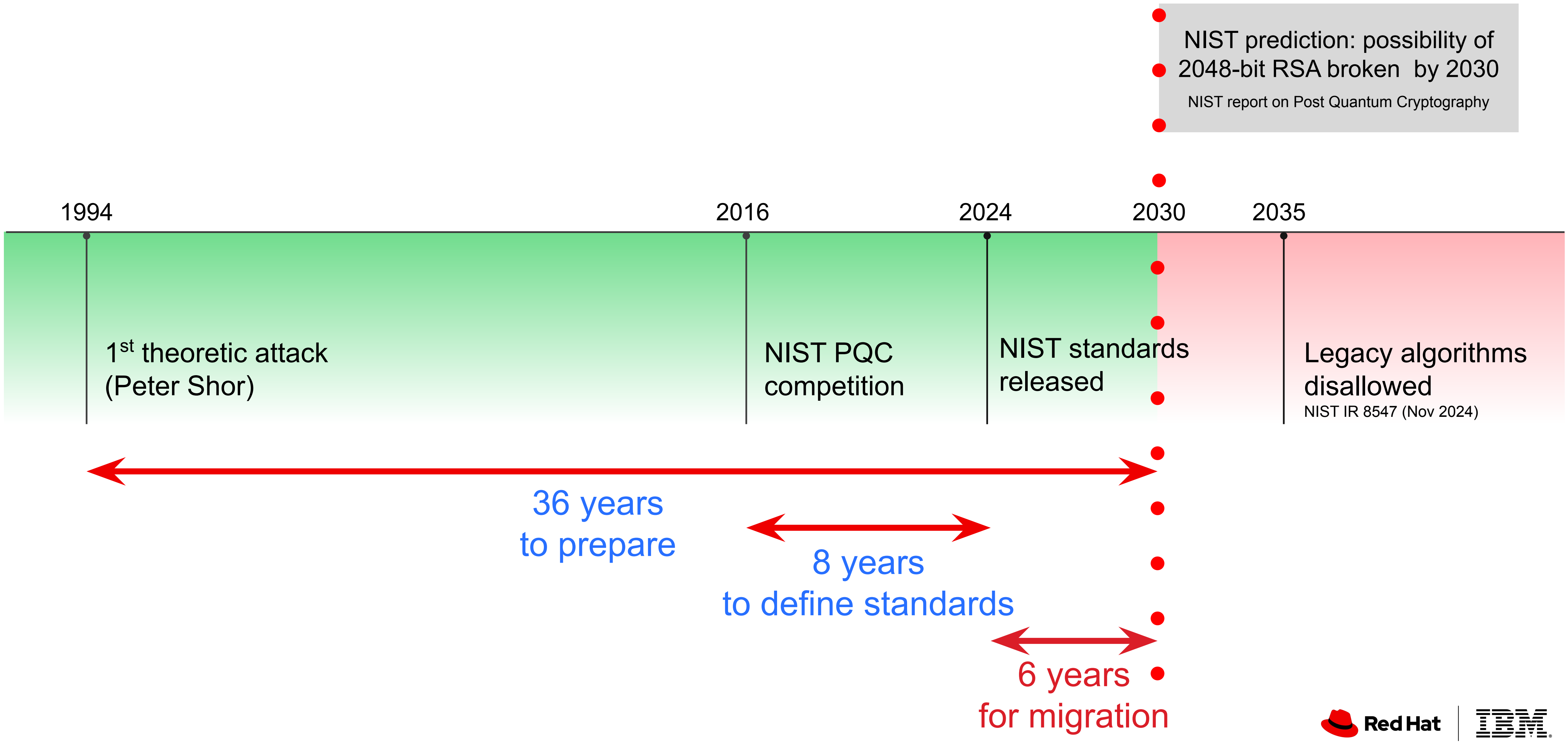
→ ML-KEM

→ ML-DSA
→ FN-DSA
→ SLH-DSA

IBM Research Zurich and partners

Red Hat | IBM

Quantum Safe Cryptography and Migration



NIST prediction: possibility of 2048-bit RSA broken by 2030

NIST report on Post Quantum Cryptography

1994

1st theoretic attack (Peter Shor)

2016

NIST PQC competition

2024

NIST standards released

2030

2035

Legacy algorithms disallowed

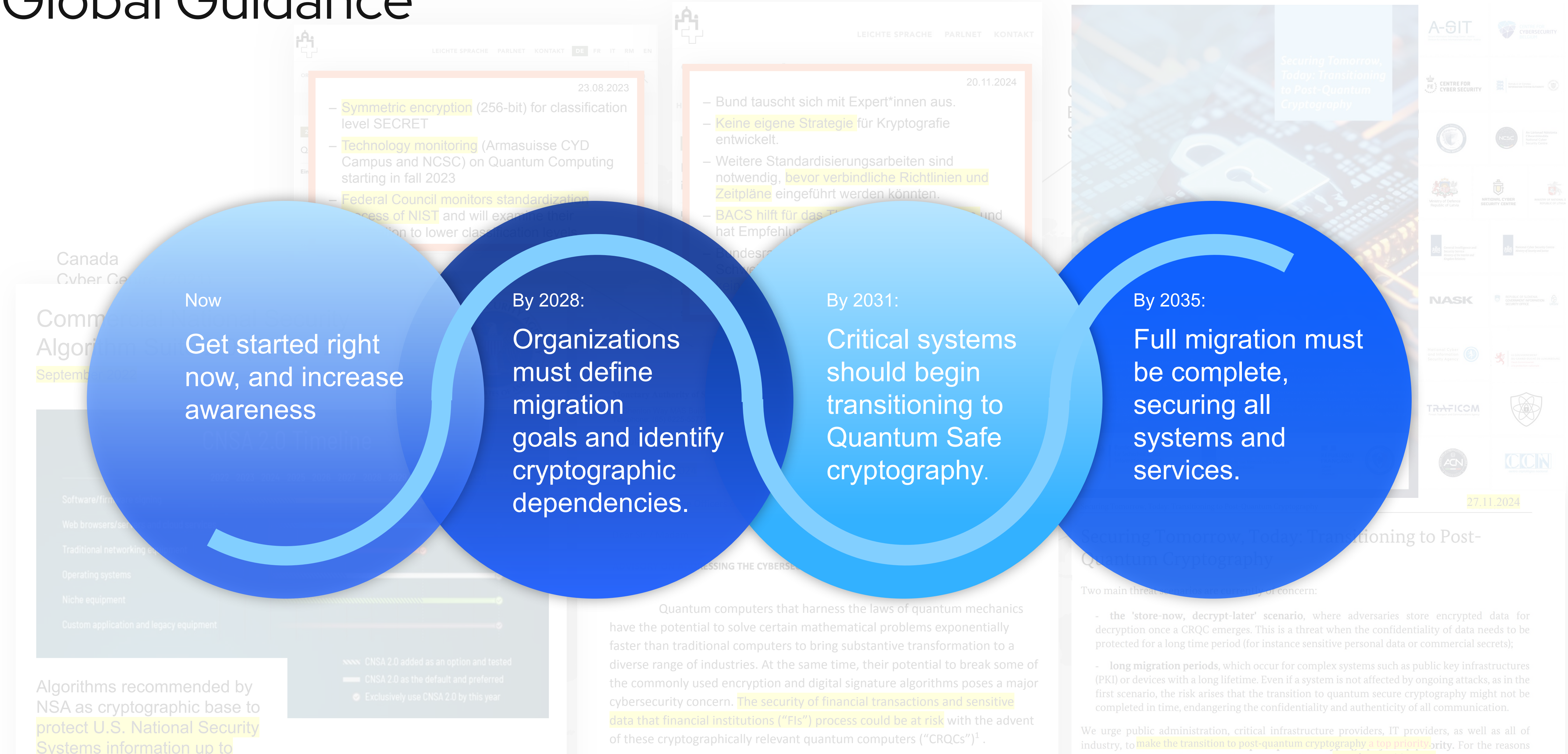
NIST IR 8547 (Nov 2024)

36 years to prepare

8 years to define standards

6 years for migration

Global Guidance



Now

Get started right now, and increase awareness

By 2028:

Organizations must define migration goals and identify cryptographic dependencies.

By 2031:

Critical systems should begin transitioning to Quantum Safe cryptography.

By 2035:

Full migration must be complete, securing all systems and services.

23.08.2023

- Symmetric encryption (256-bit) for classification level SECRET
- Technology monitoring (Armasuisse CYD Campus and NCSC) on Quantum Computing starting in fall 2023
- Federal Council monitors standardization process of NIST and will examine their application to lower classification levels

20.11.2024

- Bund tauscht sich mit Expert*innen aus.
- Keine eigene Strategie für Kryptografie entwickelt.
- Weitere Standardisierungsarbeiten sind notwendig, bevor verbindliche Richtlinien und Zeitpläne eingeführt werden könnten.
- BACS hilft für das Th… und hat Empfehlun…

Canada Cyber Ce…

Comm… Algorithm Sui…

September 2022

CNSA 2.0 Timeline

Software/firmware signing

Web browsers/servers and cloud services

Traditional networking equipment

Operating systems

Niche equipment

Custom application and legacy equipment

CNSA 2.0 added as an option and tested

CNSA 2.0 as the default and preferred

Exclusively use CNSA 2.0 by this year

Algorithms recommended by NSA as cryptographic base to protect U.S. National Security Systems information up to the top-secret level.

…SSING THE CYBERSE…

Quantum computers that harness the laws of quantum mechanics have the potential to solve certain mathematical problems exponentially faster than traditional computers to bring substantive transformation to a diverse range of industries. At the same time, their potential to break some of the commonly used encryption and digital signature algorithms poses a major cybersecurity concern. The security of financial transactions and sensitive data that financial institutions ("FIs") process could be at risk with the advent of these cryptographically relevant quantum computers ("CRQCs")[1].

https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/ma… quantum-advisory.pdf

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography

A-SIT

NASK

TRAFICOM

CCN

27.11.2024

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography

Two main threat scenarios are currently of concern:

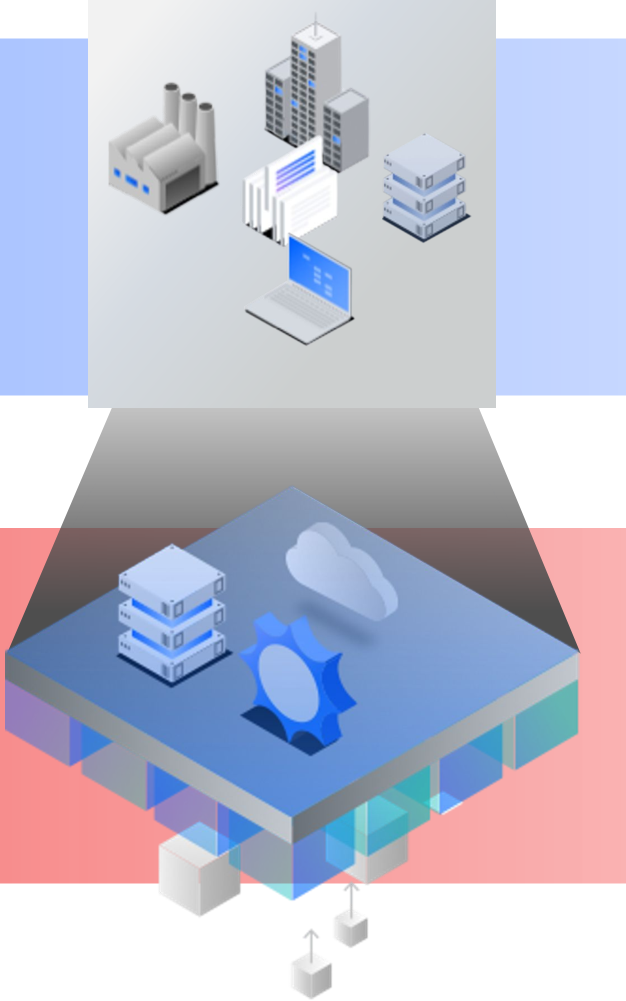
- the 'store-now, decrypt-later' scenario, where adversaries store encrypted data for decryption once a CRQC emerges. This is a threat when the confidentiality of data needs to be protected for a long time period (for instance sensitive personal data or commercial secrets);
- long migration periods, which occur for complex systems such as public key infrastructures (PKI) or devices with a long lifetime. Even if a system is not affected by ongoing attacks, as in the first scenario, the risk arises that the transition to quantum secure cryptography might not be completed in time, endangering the confidentiality and authenticity of all communication.

We urge public administration, critical infrastructure providers, IT providers, as well as all of industry, to make the transition to post-quantum cryptography a top priority. For the reasons outlined above, organizations and governments should start the transition now by working on the following steps (we refer to [5] and [6] for more details):

Timeline from UK NCSC (March 2025)

https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

Breaking down the challenge:
How to discover cryptography and become quantum safe?



Enterprise Cryptographic Posture

"Things that I use"

- Software
- SaaS
- Network
- Documents
- PKI
- Data
- Devices/IoT

CIO / CISO / CTO

Line of Business

App & Product Cryptographic Posture

"Things that I control"

- Applications
- Source code
- Platforms
- Software dependencies
- Configuration

Product Owners

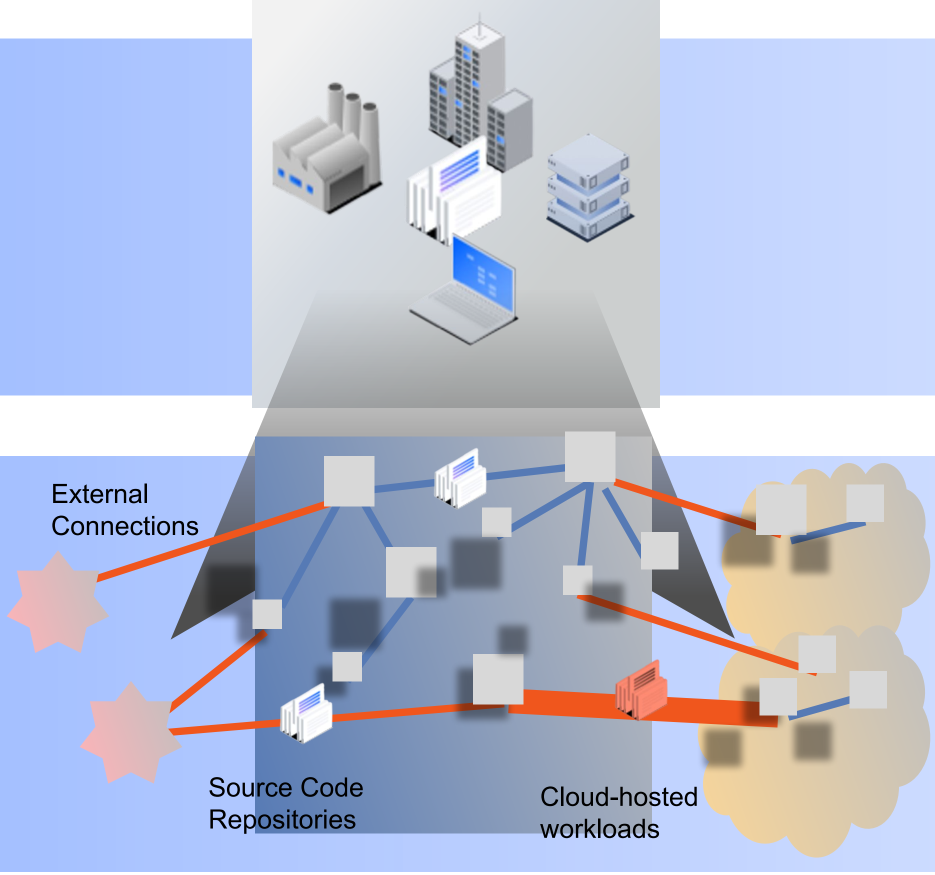
Developers

Breaking down the challenge:
How to discover cryptography and become quantum safe?

Enterprise Cryptographic Posture

“Things that I use”

Dependencies and Risks



⚠ No cryptographic inventory available

Optimized change management

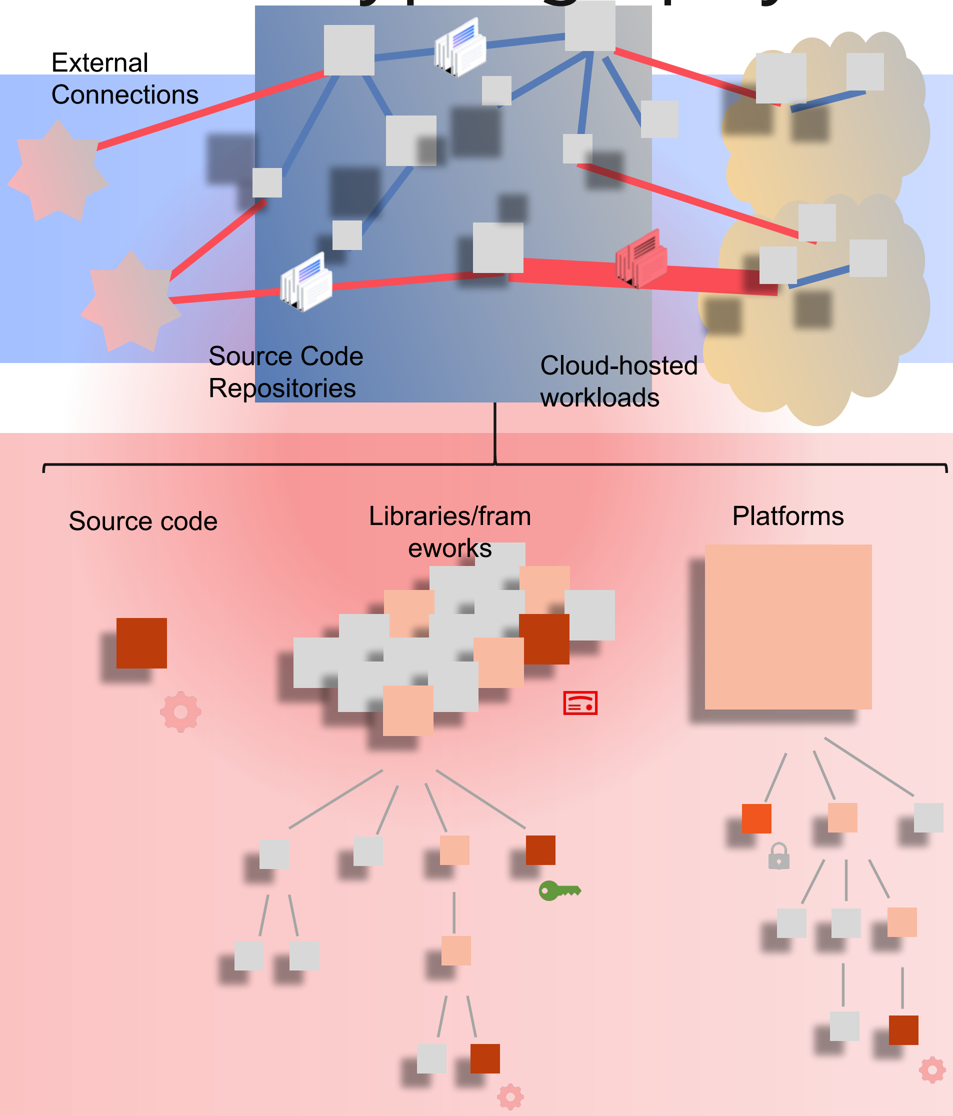
Urgent actions – Modernization - Vendors

IBM Research

Active research on innovations and technologies to optimize and orchestrate migration.

Breaking down the challenge:
How to discover cryptography and become quantum safe?

Dependencies and Risks



App & Product Cryptographic Posture

No organization has access to all source code in use

Exchange information about cryptography

IBM Research

CBOM

Cryptography Bill of Materials (CBOM)

OWASP CycloneDX 1.7, ECMA Standard

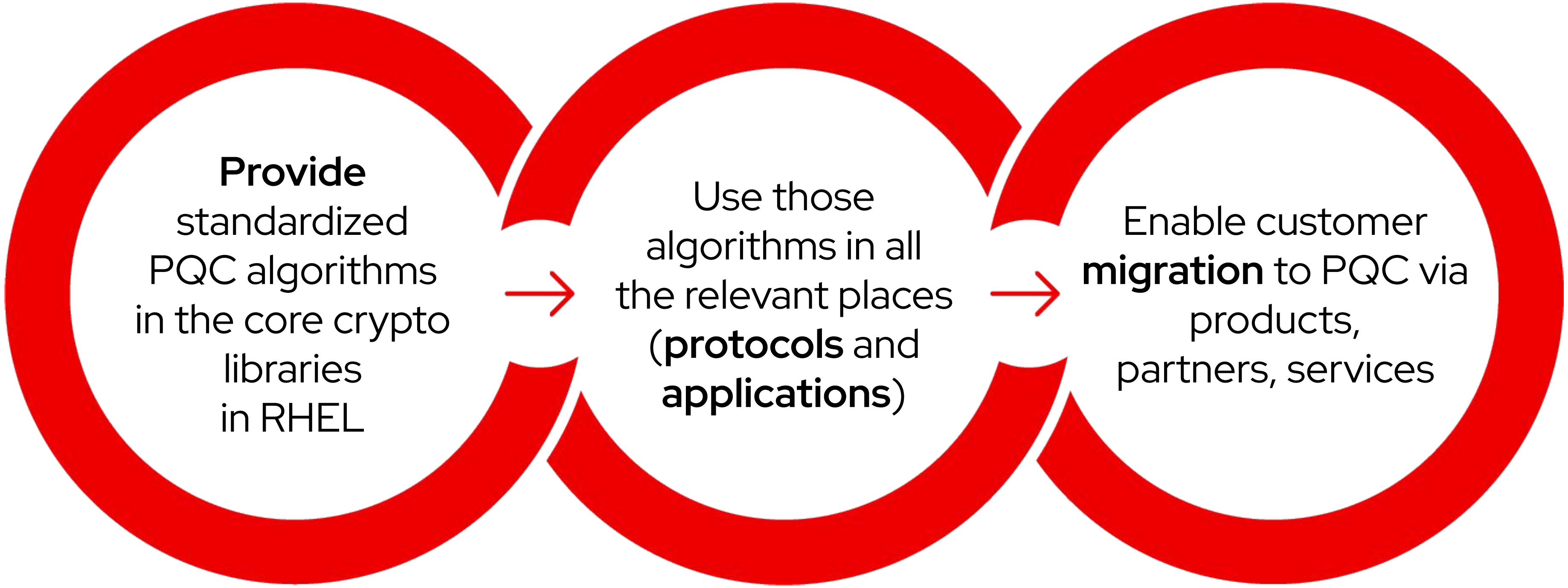
OWASP

THE LINUX FOUNDATION

Post-Quantum Cryptography Alliance

Red Hat’s basic strategy

How we will execute the shift to PQC



Provide standardized PQC algorithms in the core crypto libraries in RHEL

→

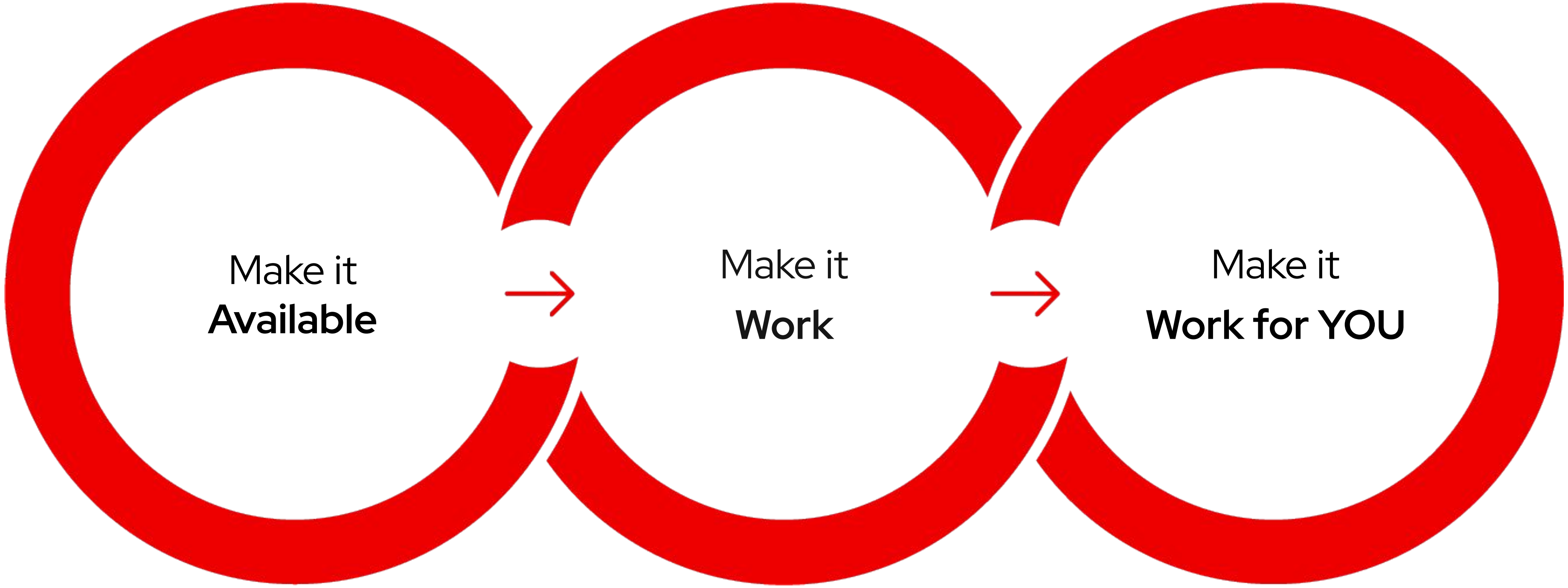
Use those algorithms in all the relevant places (**protocols** and **applications**)

→

Enable customer **migration** to PQC via products, partners, services

What does this mean?

This is a journey that will prepare you for the advent of Quantum Computing



Make it
Available

→

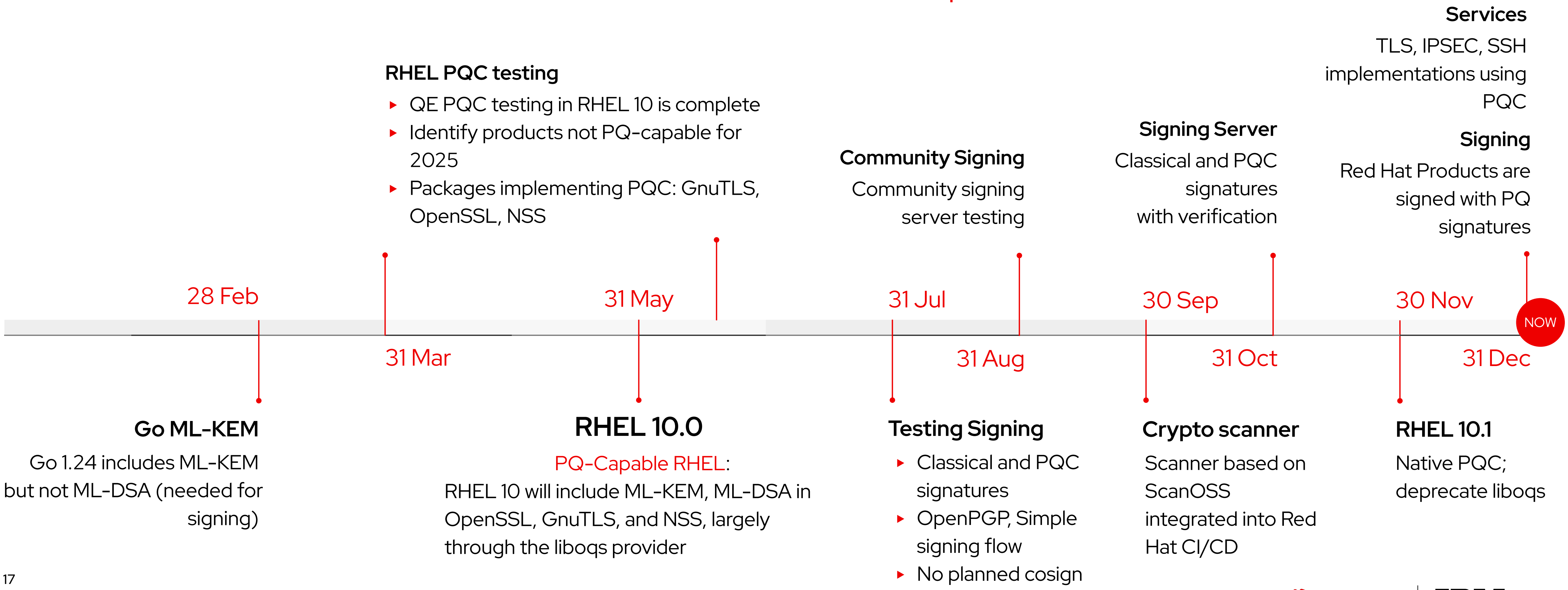
Make it
Work

→

Make it
Work for YOU

Red Hat timeline 2025

Introduction of PQC for the Red Hat portfolio



28 Feb

Go ML-KEM

Go 1.24 includes ML-KEM but not ML-DSA (needed for signing)

31 Mar

RHEL PQC testing

- QE PQC testing in RHEL 10 is complete
- Identify products not PQ-capable for 2025
- Packages implementing PQC: GnuTLS, OpenSSL, NSS

31 May

RHEL 10.0

PQ-Capable RHEL:
RHEL 10 will include ML-KEM, ML-DSA in OpenSSL, GnuTLS, and NSS, largely through the liboqs provider

31 Jul

Testing Signing

- Classical and PQC signatures
- OpenPGP, Simple signing flow
- No planned cosign

31 Aug

Community Signing

Community signing server testing

30 Sep

Crypto scanner

Scanner based on ScanOSS integrated into Red Hat CI/CD

31 Oct

Signing Server

Classical and PQC signatures with verification

30 Nov

RHEL 10.1

Native PQC; deprecate liboqs

31 Dec

Signing

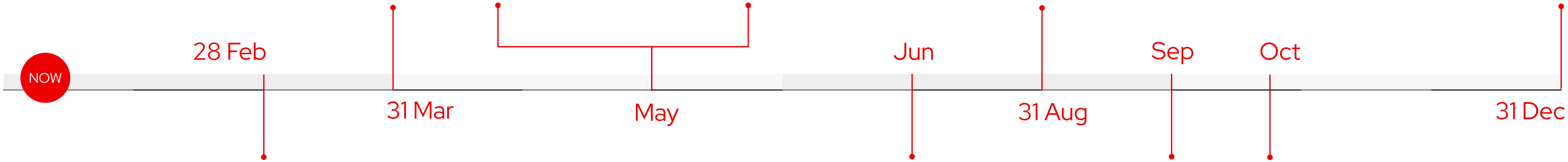
Red Hat Products are signed with PQ signatures

Services

TLS, IPSEC, SSH implementations using PQC

Red Hat timeline 2026

Diffusion of initial PQC across the Red Hat portfolio



TBD

RHEL 10.x

- Python PQC added
- ML-KEM in libreswan for IPSec support

AAP Core

- PQC-enabled Python base; TLS 1.3 hybrid certificates and ssh
- Dual verification of classical & PQC signatures on RPMs and container images

OCP

- PQC KEM w/ TLS 1.3 for OCP Core Components
- Connect to OCP w/ Hybrid PQC OpenSSH
- OpenSSL 3.5 supports PQC for use by operators

Layered Products

Select product on select versions of RHEL use TLS 1.3 w/ ML-KEM

Quay

- Quay now supports SHA-512

OCP

- OCP platform integrates RHEL PQC capability OpenShift layered operators that use go/crypto are re-built using PQC-enabled key encapsulation (ML-KEM)

RHTAS

- QC signature hosting and serving feature is fully incorporated into RHTAS
- PQC-aware client-side verification tool

Your Migration

... or Modernization?

Inventory & Agility

- Find all crypto usage
- Standardize with CBOM
- Hybrid approach
- Crypto Agility

System & Performance

- TLS 1.3 only
- Upstream Dependencies
- No Backporting
- Test performance impact

Resources & Monitoring

- Skills & budget scarcity
- Upgrade platforms & dependencies
- Continuous monitoring

Example

Enterprise Java App

- Java 17
- TLS 1.2 (RSA/ECDHE)
- Exposes Rest Endpoint
- Hello World Logic

Migration to PQ Ready

- Java 25
- TLS 1.3 only
- Hybrid Support: Classical & PQ
- Hybrid ML-KEM
- Vulnerable to downgrade attack

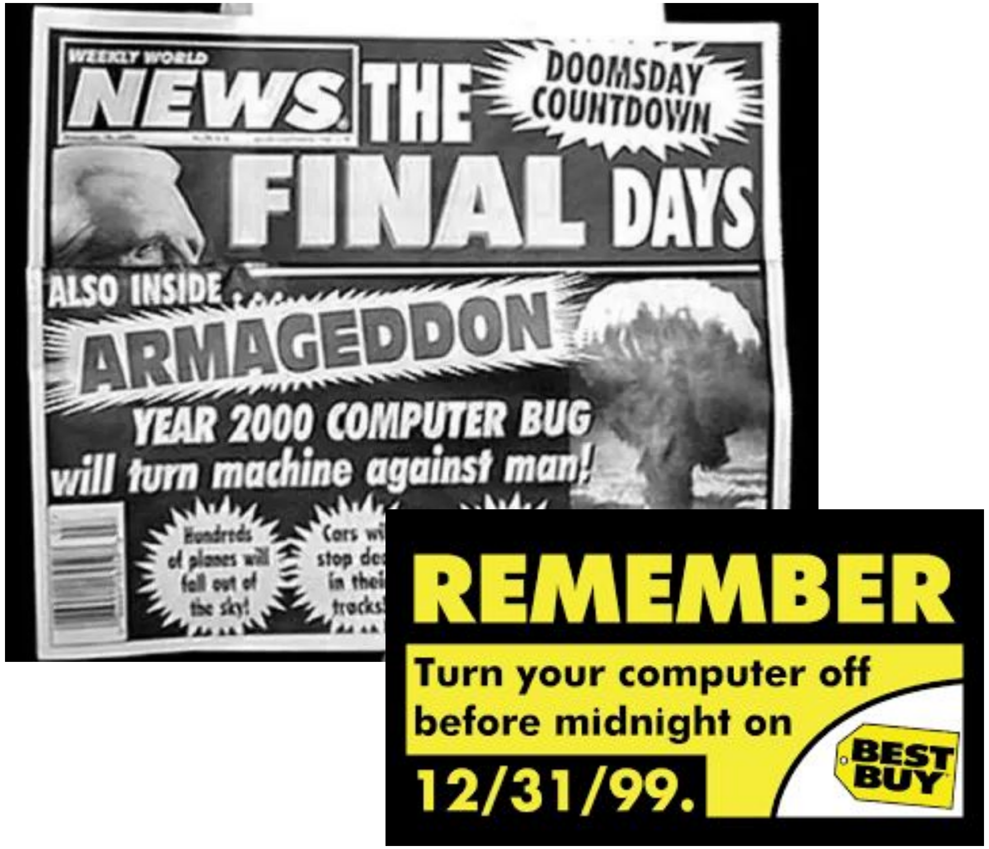
How much % of modification was needed?

Baseline LOC (main): 917
Changed LOC: 1273
Churn: 138.00%

Source:
Example Repository: https://github.com/maschind/pqc-demo/
Calculation: scripts/calc-change.sh

TL;DPA

Too Long; Didn’t Pay Attention



WEEKLY WORLD NEWS

DOOMSDAY COUNTDOWN

THE FINAL DAYS

ALSO INSIDE

ARMAGEDDON

YEAR 2000 COMPUTER BUG will turn machine against man!

Hundreds of planes will fall out of the sky!

Cars wi stop de in thei tracks!

REMEMBER

Turn your computer off before midnight on 12/31/99.

BEST BUY

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat