IBM Quantum Safe Infrastructure

Zaščita podatkov v dobi kvantnega računalništva

David Kosmač
Infrastructure Technical Sales Leader,
Central and Eastern Europe Territories

IBM **Quantum** Safe

Our mission

→ Bring useful quantum computing to the world

→ Make the world quantum safe

Our modern digital world depends on cryptography

And quantum computing is ushering in a new cryptographic era

Prime factors

= p x q

2048-bit composite integer

25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564392120103971228221207203570

Expected computation time

The most powerful computer **today:**

Millions of years

Shor’s quantum algorithm:

Hours

Public key encryption • Digital signatures • Key exchange algorithms

RSA • DSA • ECC • ECDSA • DH

What are cybercriminals doing now?

Harvest now, decrypt later

Now

Harvest confidential data to decrypt later

Availability of “cryptographically relevant” quantum computers

Later

Decrypt lost or harvested confidential data by breaking encryption

Disrupt business with manipulation through fraudulent authentication

Manipulate digitally signed contracts and legal history by forging digital signatures

Our digital world depends on cryptography, which is used in trillions of transactions on billions of devices

Internet
- Domain name system (DNS)
- Hypertext transfer protocol (HTTP)
- File transfer protocol (FTP)

Digital signatures
- Electronic identification and trust services (eIDAS)
- PDF advanced electronic signature (PAdES)
- Advanced electronic signatures

Critical infrastructure
- Code updates
- Control systems
- Car systems

Financial systems
- Payment systems

Enterprise
- Email
- Identity management
- LDAP
- PKI services
- Bespoke applications

Documents that needs to stay secure for a long period of time

Passports: 10 years from issue

Road vehicles: 15–20 years

Aircraft/rail: 25–30 years

Some critical infrastructure: 50+ years

Data needs to stay secure for a long time

HIPAA: 6 years from last use per Security Rule

Tax records: 7–10 years in most countries; Sarbanes-Oxley Act set the precedent in the US

Legitimate interest under GDPR: 20+ years

What will a cybercriminal be able to do?

1. Harvest encrypted communications

2. Harvest encrypted keys

3. Harvest Public Keys/Certificates

“Q-Day”
availability of “cryptographically relevant” Quantum Computer

Extract Private Key from Public key

BEFORE

AFTER

DECRYPT

- Decrypt lost or harvested comms
- Decrypt current comms, data & backups
- Undo privacy in blockchains

DISRUPT

- Create fraudulent firmware updates
- Modify vulnerability scanner patterns
- Issue fraudulent blockchain transactions
- Fraudulent access to systems

MANIPULATE

- Fraudulently change historical digitally signed contracts
- Create fraudulent new contracts
- Modify signed digital evidence
- Create fraudulent digital evidence

What will a cybercriminal be able to do?

Harvest now, decrypt later

Fraudulent authentication

Forge digital signatures

Replacing most of the public key systems currently in use will take 5 to 15 years.

Data generated today that is not protected with quantum-safe cryptography is already at risk.

When would the Quantum threat **materialize?**

When is Q-Day?

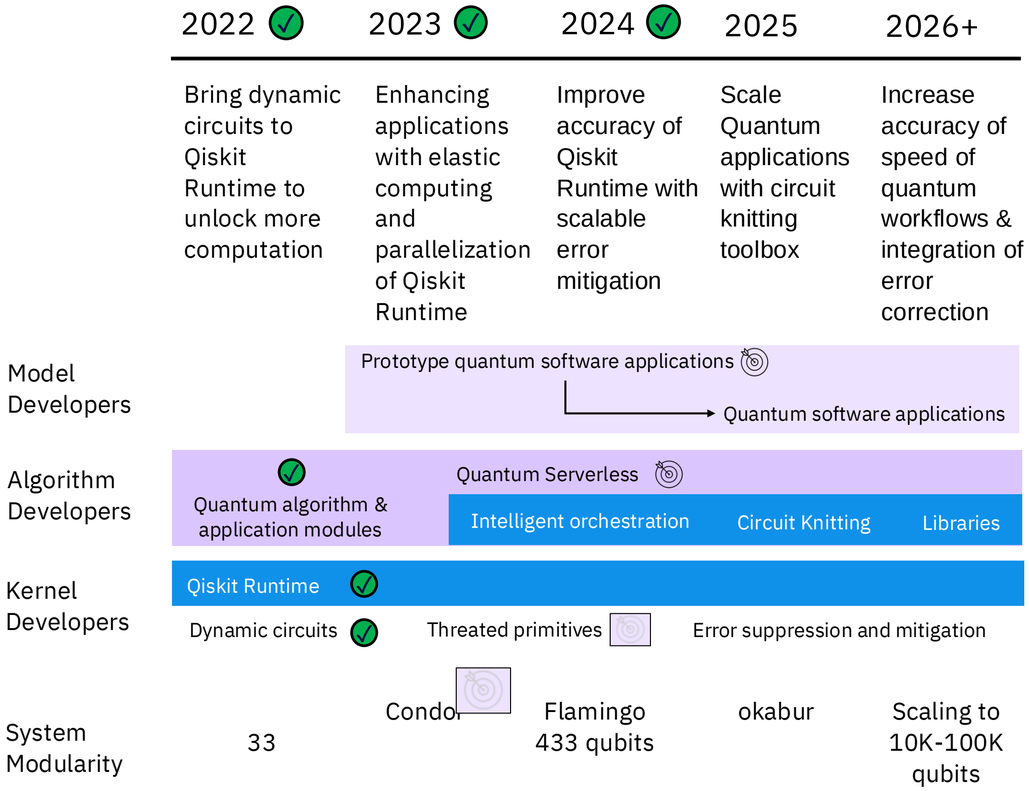
"The National Institute of Standards and Technology predicts it may be possible to break 2048-bit RSA **by 2030**

- NIST report on Post Quantum Cryptography

“There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a **1 in 2 chance** of the same **by 2031**”

- Dr. Michele Mosca, Institute of Quantum Computing,
University of Waterloo

Quantum Computing Status and Roadmap



13,426* physical Qubits Required
to break RSA 2048

Elliptic Curve Cryptography (ECC) requires fewer logical Qubits – likely to be at risk earlier

The **good news**

1

Quantum safe cryptography exists and gets standardized

2

Governments issue advisories and directives

3

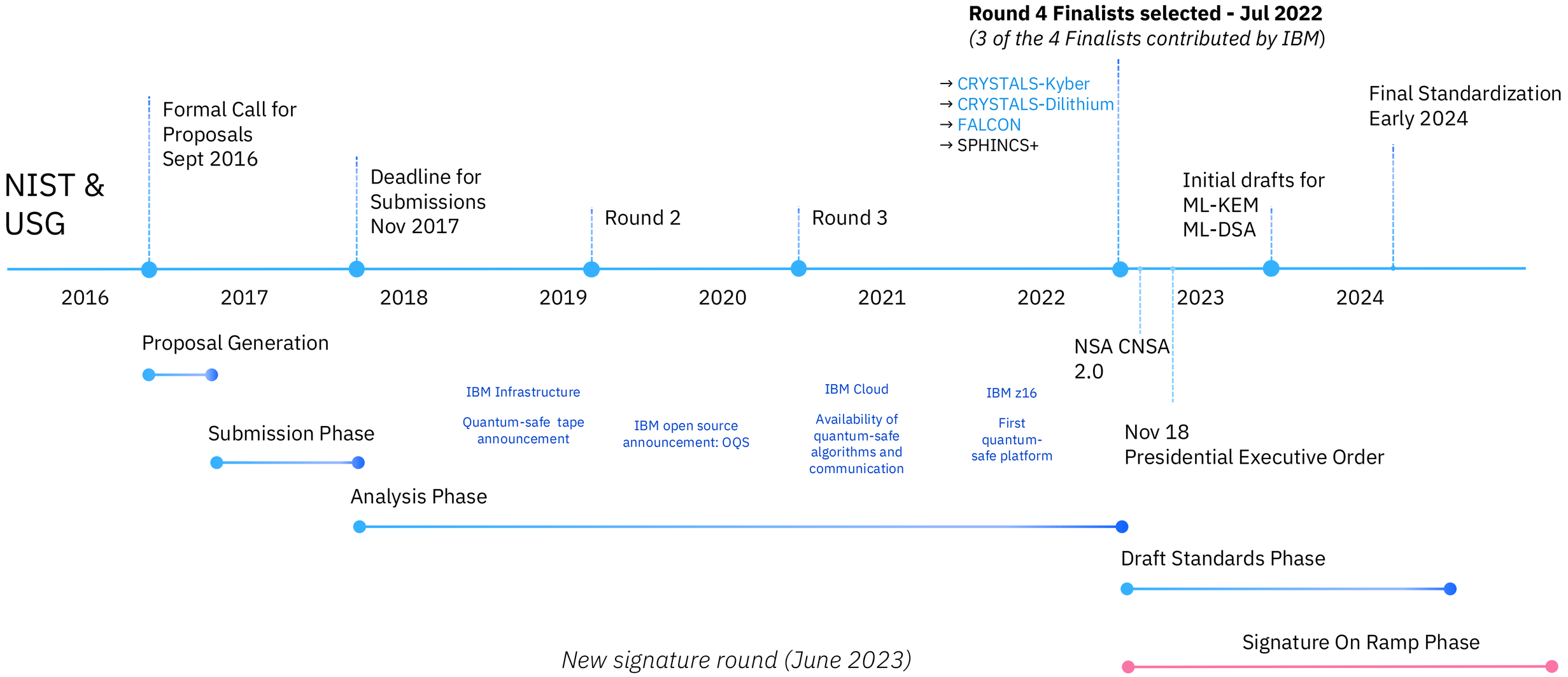
Awareness of the extent and urgency is growing

… and first quantum-safe systems are already available!

(*) arxiv.org/pdf/2103.06159.pdf

Quantum Safe Cryptography

NIST standardization for Quantum Safe Cryptography



NIST to standardize PQC finalists

Three of the four algorithms announced by NIST were created by IBM in partnership with industry and academia[2]:

CRYSTALS-Kyber (ML-KEM)

- KEM based on structured lattices
- Good all-around performance and security

CRYSTALS-Dilithium (ML-DSA)

- Digital signature based on structured lattices
- Good all-around performance and security; relatively simple implementation

Falcon (FN-DSA)

- Digital signature based on structured lattices
- Smaller bandwidth, but much more complicated implementation
- The Falcon standard will come out after the others

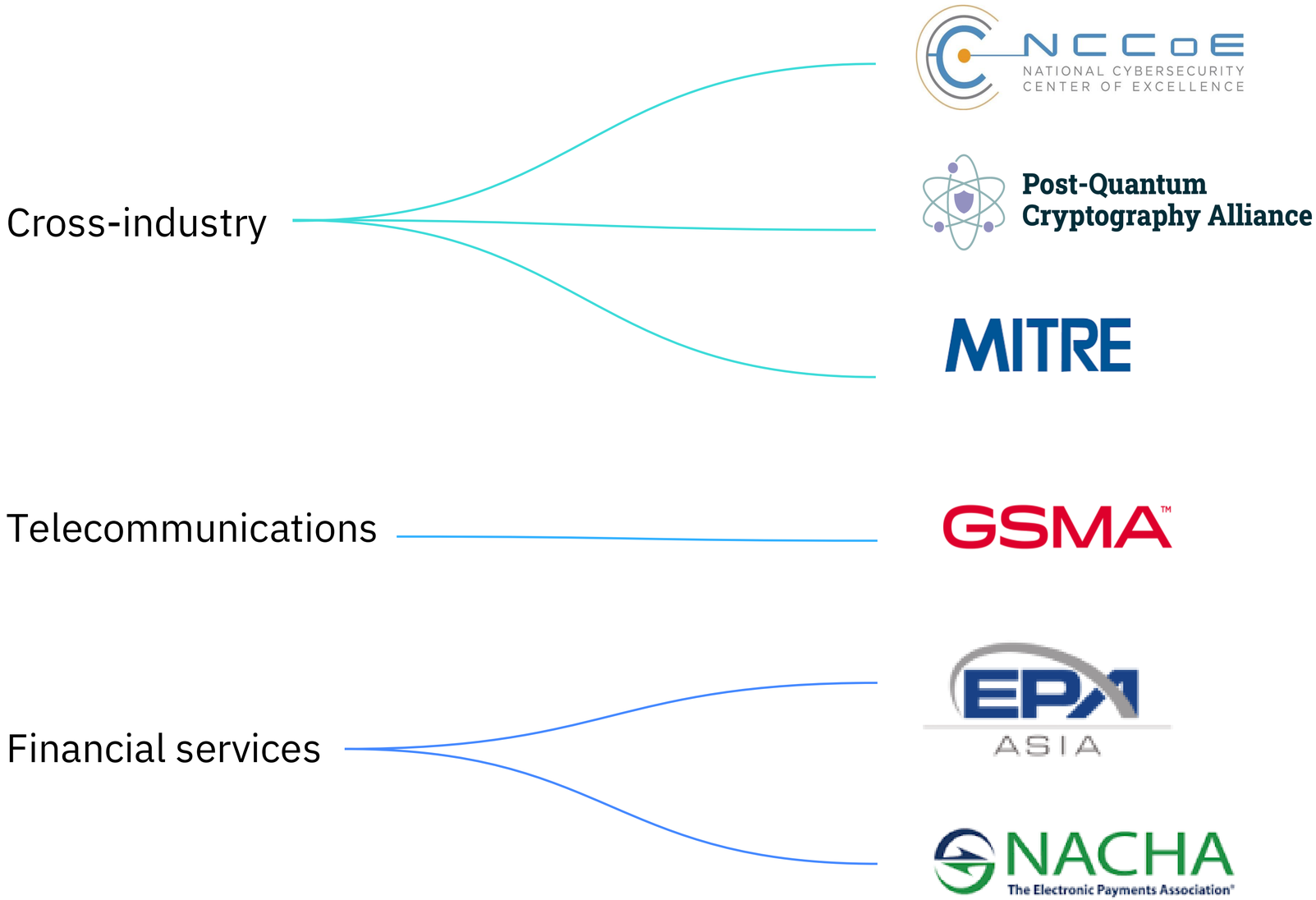
SPHINCS+ (SLH-DSA)

- Digital signature based on stateless hash-based cryptography
- Solid security, but performance is not as good as CRYSTALS-Dilithium and Falcon

[2] "NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers," 24 August 2023.

IBM moving the quantum-safe ecosystem forward

↳ Open-source projects
↳ Centers of excellence
↳ Industry consortia



Awareness and urgency are growing

Apple’s iOS 17.4 includes cryptographic protocol in iMessage

Introducing post-quantum cryptography from the start of a conversation so that all communication is protected from current and future adversaries.

Using a hybrid design to combine new post-quantum algorithms with current algorithms

Source

Google advances quantum-resistant cryptography efforts in Chrome browser

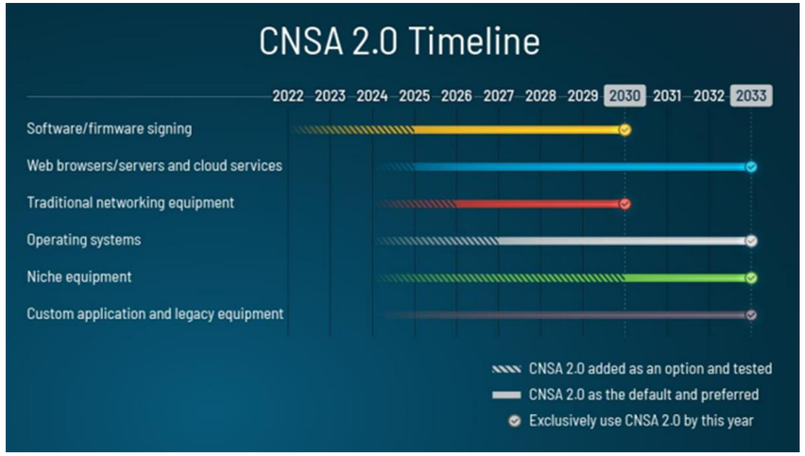
Google is recognizing the risk of the “harvest now, decrypt later” threat and addressing issues of post-quantum security by updating standards and testing new quantum-resistant algorithms.

Source

US Government mandate for quantum-safe federal agencies

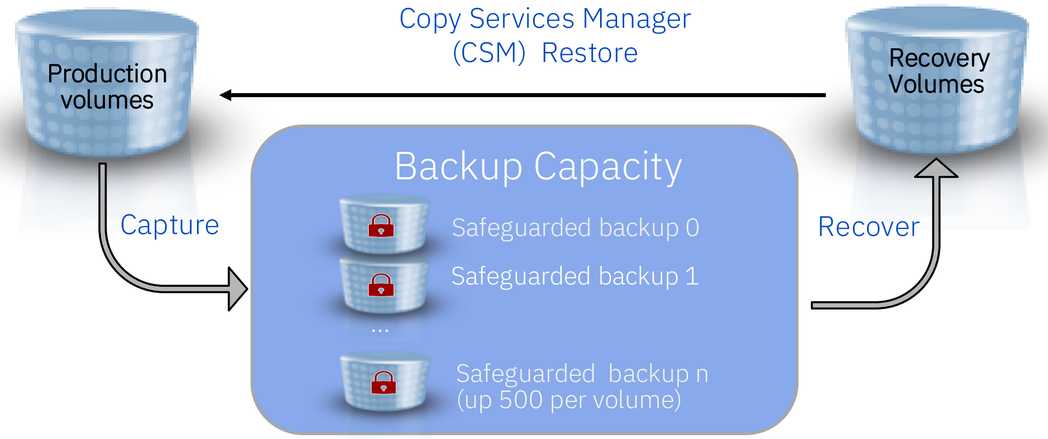
CNSA 2.0: Quantum-safe standards are preferred for national security systems by the mid-2020s and required by the early 2030s to defend against threats.

Source



IBM Power Integrated with IBM Storage for Cyber-Resilient Recovery and Encryption

- Security PINS are sent to the drive in encrypted form over PCI bus with secure key passing (SKP)
- Flash Core Module: FCM 4
  - FIPS 140-3-Level 2 in process
  - RSA and CRYSTALS Kyber Quantum Safe Algorithms
  - SKP is encrypted twice, once by each cypher



IBM Storage provides **Safeguarded Copy**

Validation

Forensic Analysis

Surgical Recovery

Catastrophic Recovery

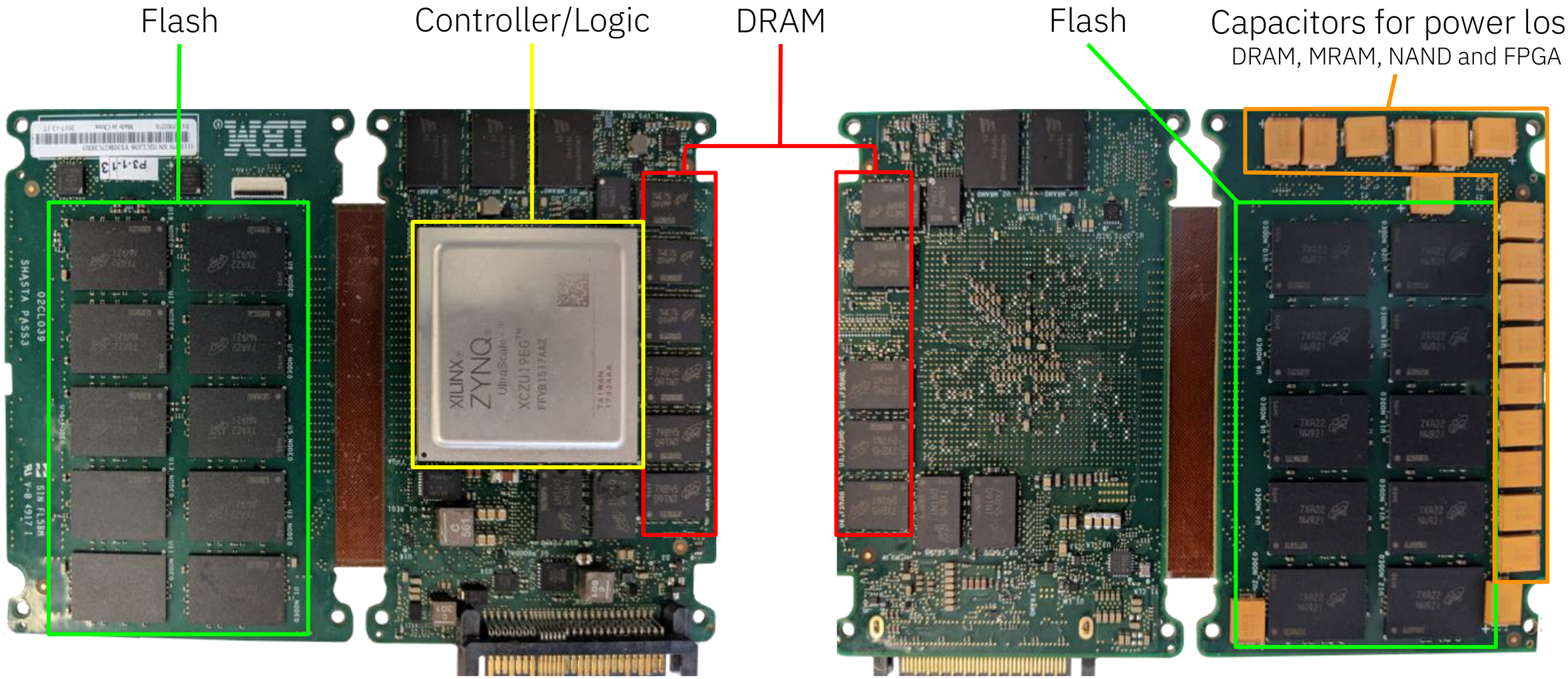
Offline Backups

IBM Storage with Safeguarded Copy provides immutable, consistent point-in-time copies of data.

CSM manages the creation, recovery, and restoration of the copies and provides automation to manage those processes.

IBM Power hardware and software provides a secure, isolated environment to perform data validation, forensic analysis, and create offline backups.

FlashCore Modules are Computational Storage Devices



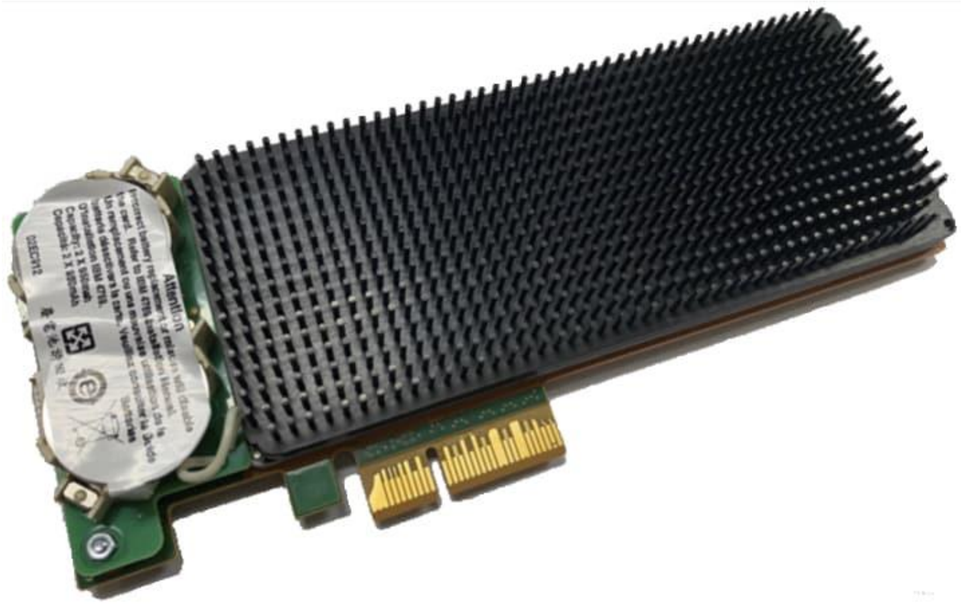
FlashCore Modules are Quantum Safe, SSDs not so much

Abilities	FCM	SSD
Built-in Quantum Safe Encryption	✓	✗
Extensive Built-in Compression	✓	?
Extensive Health Binning	✓	✗
Extensive Heat Segregation	✓	✗
Variable Voltage	✓	✗
Variable Stripe RAID (Intra Module RAID)	✓	✗
~70µs latency	✓	✗
Ransomware Threat Detection	✓	✗

FCMs use hybrid implementation of asymmetric cryptography including QSC cryptographic algorithms:

- CRYSTALS-Dilithium signatures for authentication and firmware verification
- CRYSTALS-Kyber for secure key transport of unlock PIN transmitted by FlashSystem storage controller to FCM

Hardware security protection for sensitive data with NextGen IBM Crypto Express Card (4769)



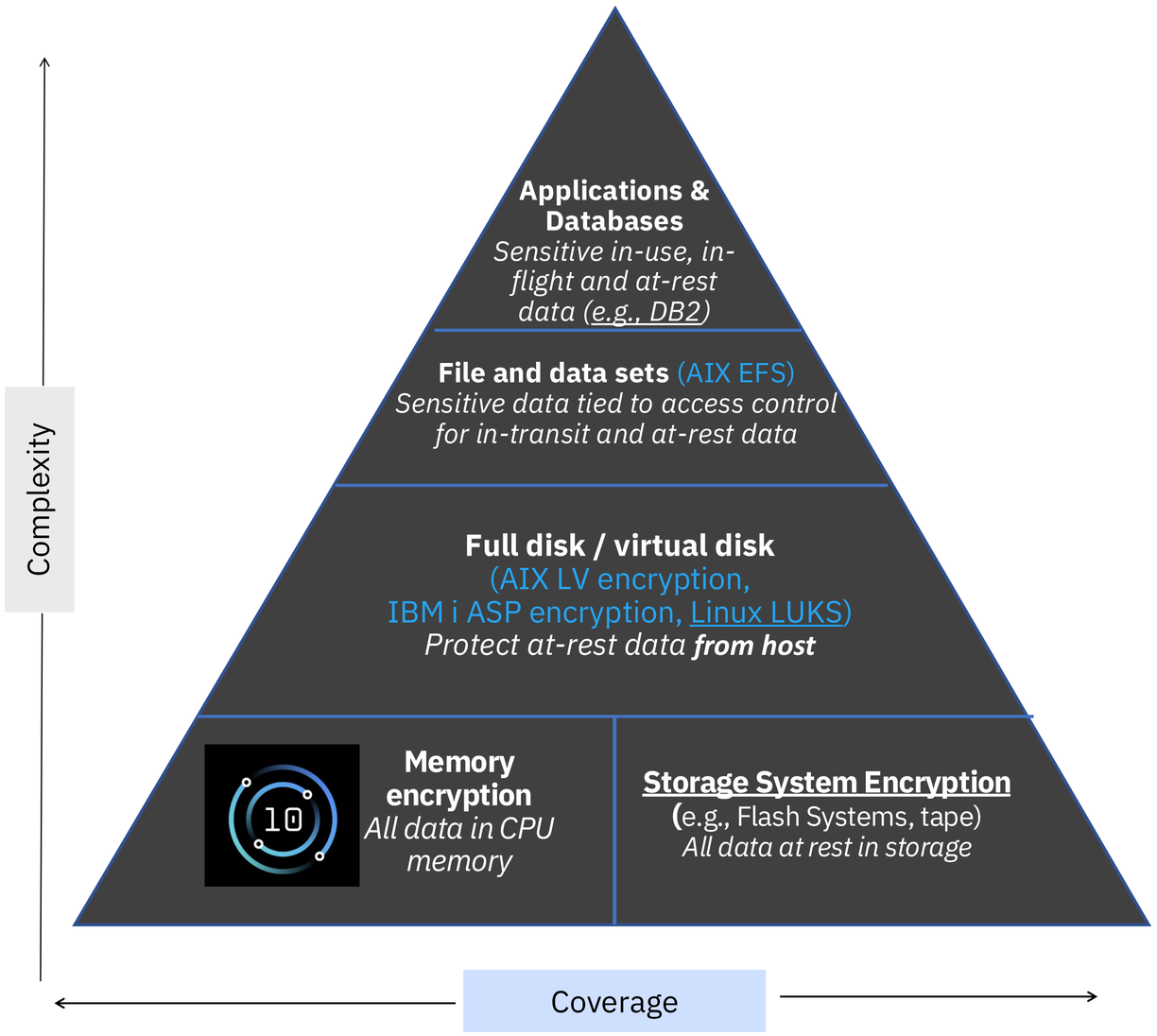
- Hardware Security Module (HSM) for highest security, especially where tamper protection is required
- Complementary to Power10 Core Cryptographic acceleration
- Validated to U.S. NIST FIPS 140-2/3 Standards Overall Security Level 4

Next generation card, 4769

- Available on IBM Power10® servers, either on AIX®, IBM i®, or PowerLinux™ and IBM Power9® servers, either on AIX or IBM i

Data Protection Pyramid w. Power10

End to end security with full stack encryption, in transit, at rest, in memory



Transparent memory encryption with:

- No additional management setup
- No performance impact

Blazing fast hardware-accelerated encryption compared to Power9

- 4X crypto engines in every core
- 2.5X faster AES crypto performance per core*
- Encrypted Live Partition Mobility (LPM)

Stay ahead of current and future threats with support for:

- Quantum-safe cryptography
- Fully homomorphic encryption
- Support for next generation Crypto Express Card

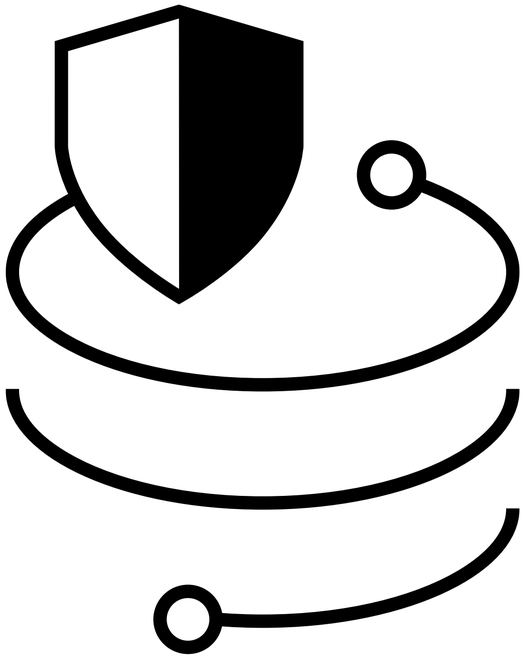
**AES-256 in both GCM and XTS modes runs about 2.5 times faster per core than comparable Power9 systems according to preliminary measurements obtained on RHEL Linux 8.4 and the OpenSSL1.1.1g library*

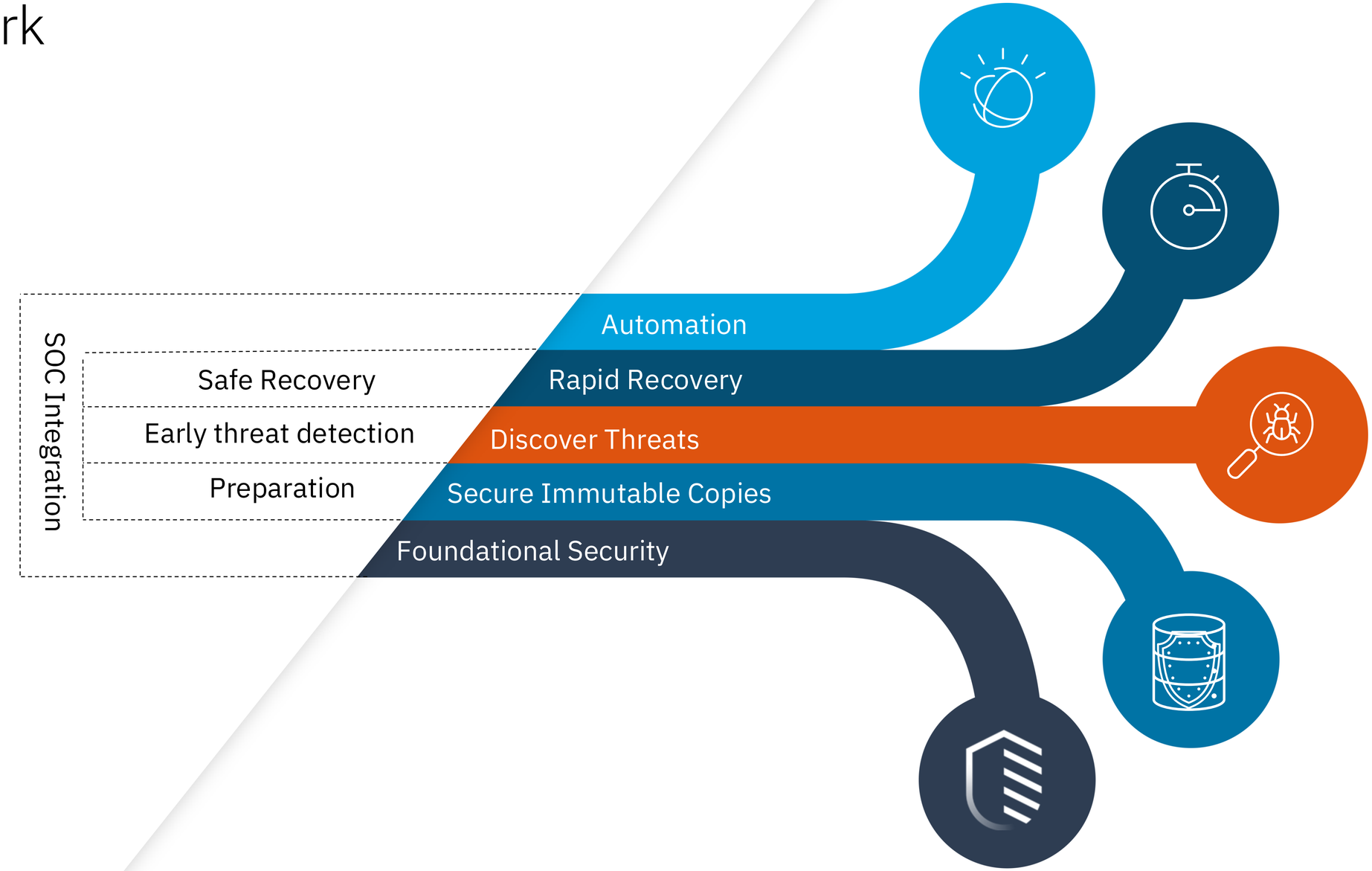
Quantum Safe Cryptography Hill: Power Roadmap (*Draft, Subject to Change*)

	Today: Power9 and Power10 Systems	Power11	Beyond Power11
Operating Systems, Workloads + Discovery	**LibOQS PoC: Tested on Power10** • **OpenSSL, OpenVPN** • **OpenSSH, cURL** • **Haproxy, Ngnix** **Cryptographic Bill of Materials (CBOM) PoC**		**QSA Enhancements of OS Cryptographic Libraries (IBM & O.S.)** **Hybrid OS quantum safe boot**
Platform: Processor + Firmware	**Efficient support of PQC algorithms (see publications)**	• **Hybrid host processor secure boot** • **LPM encryption protocol PQC support**	• **Additional in-core PQC algorithm acceleration**
Platform: Crypto Express Card (HSM)	**IBM 4769 w. Dilithium round 2 support**	**IBM 4770 w. Dilithium + Kyber pre-standard support**	

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only

Data Resiliency is like strength training. Takes building muscle and team work



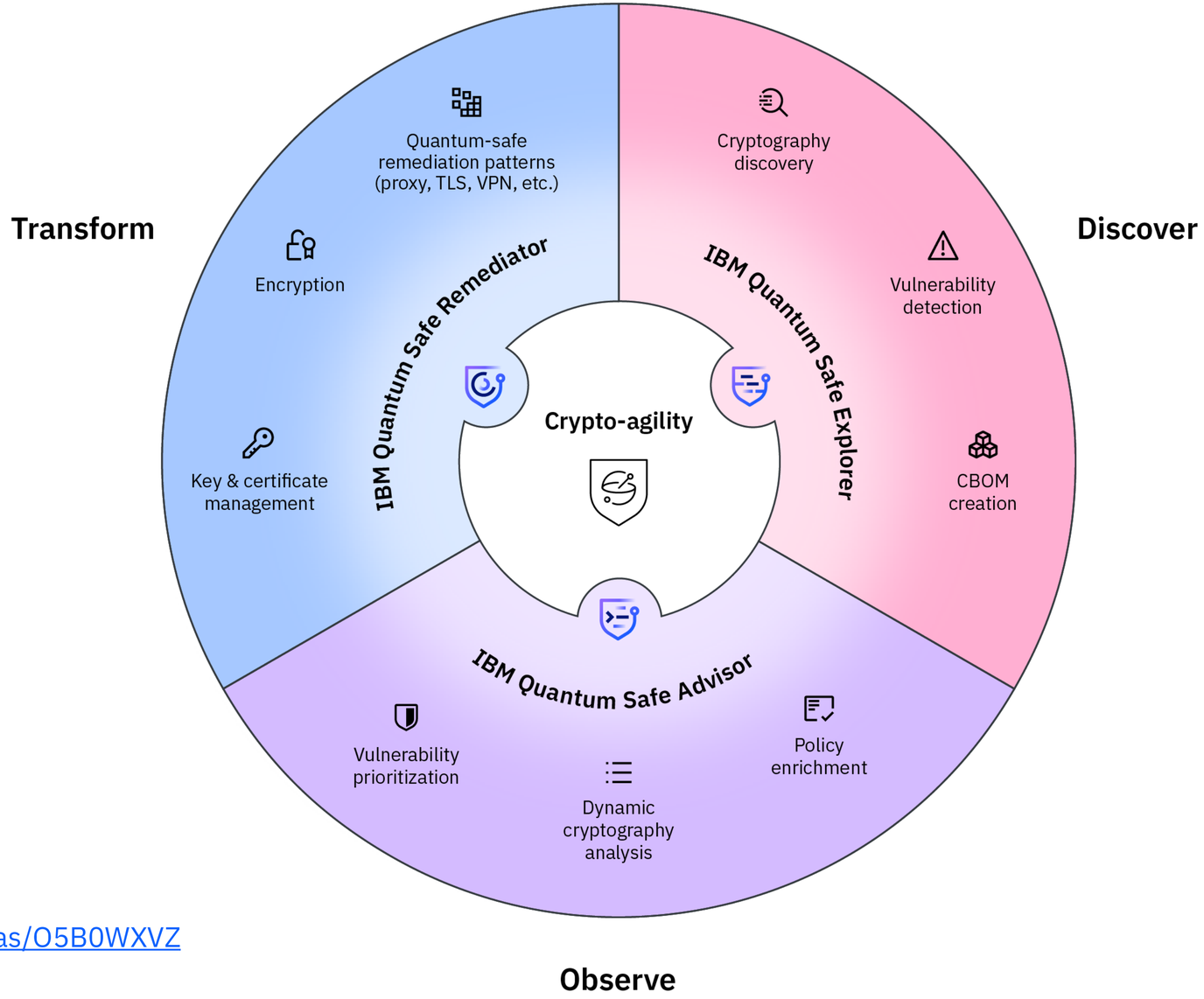


Technology and expertise powering client engagements

IBM Quantum Safe Explorer
Scan applications to locate cryptographic artifacts and vulnerabilities. Create various cryptographic inventory reports, including a Cryptography Bill of Materials (CBOM).

IBM Quantum Safe Advisor
Perform dynamic cryptography analysis to evaluate cryptographic posture and compliance. Prioritize vulnerabilities for quantum-safe transformation.

IBM Quantum Safe Remediator
Learn and apply best practices for quantum-safe remediation patterns. Implement scalable and automated quantum-safe solutions to establish cryptographic agility.



More information available at: https://www.ibm.com/downloads/cas/O5B0WXVZ

The time to start is now

Understand the quantum risks and quantum-safe priorities

Identify cryptography footprint and prioritize actions

Initiate and implement a quantum-safe program

Questions and Answers

Notices and disclaimers

This document is distributed “as is” without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM.

Not all offerings are available in every country in which IBM operates.

Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at: www.ibm.com/legal/copytrade.shtml.

Certain comments made in this presentation may be characterized as forward looking under the Private Securities Litigation Reform Act of 1995.

Forward-looking statements are based on the company’s current assumptions regarding future business and financial performance. Those statements by their nature address matters that are uncertain to different degrees and involve a number of factors that could cause actual results to differ materially. Additional information concerning these factors is contained in the Company’s filings with the SEC.
Copies are available from the SEC, from the IBM website, or from IBM Investor Relations.

Any forward-looking statement made during this presentation speaks only as of the date on which it is made. The company assumes no obligation to update or revise any forward-looking statements except as required by law; these charts and the associated remarks and comments are integrally related and are intended to be presented and understood together.