Security leadership with IBM Z & IBM LinuxONE

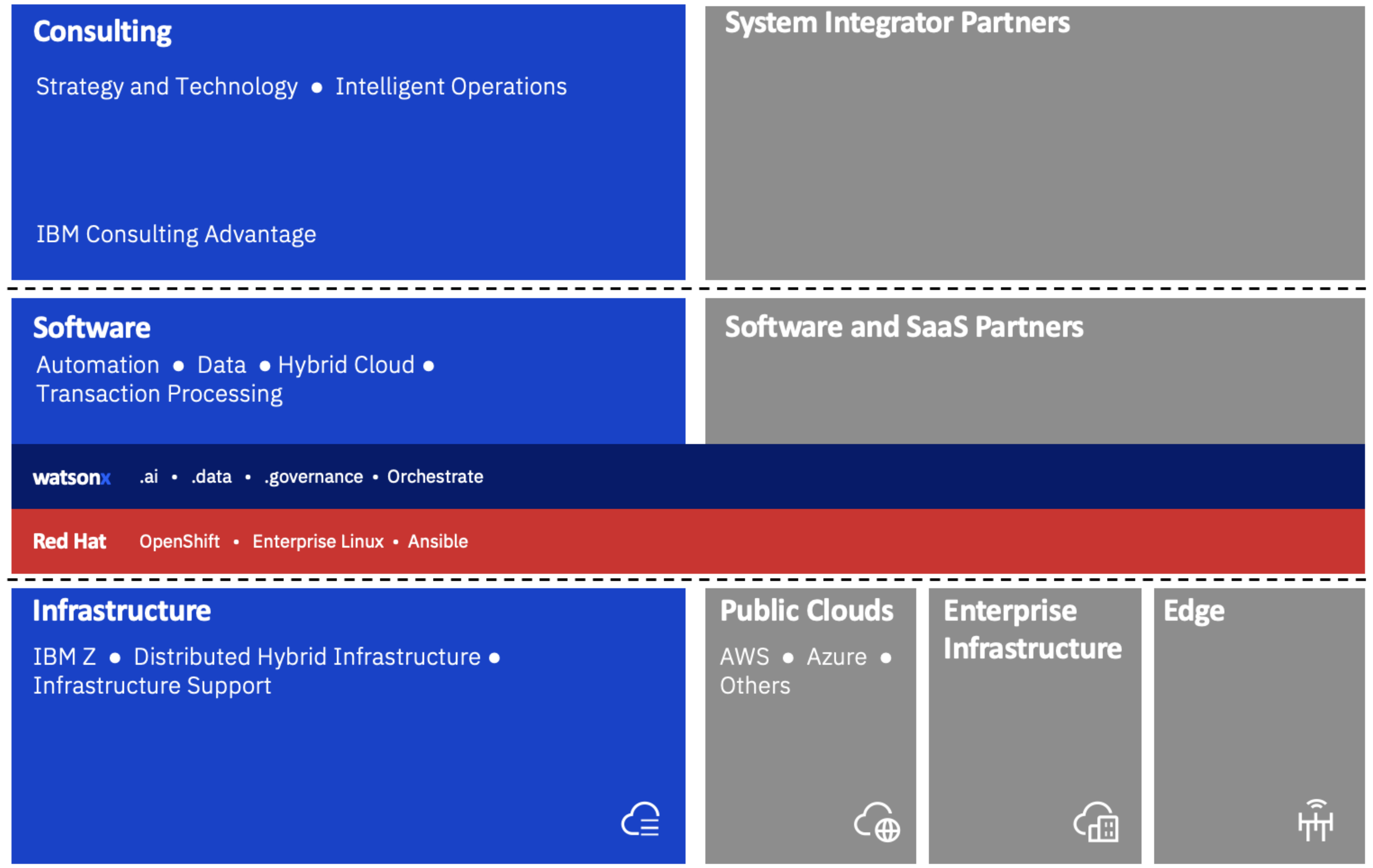
Huibert van de Putte
zStack Sales Leader
Northern, Central and Eastern Europe

Pekko Paivarinta
zStack Technical Sales Leader
Northern, Central and Eastern Europe

IBM in a glance

Hybrid cloud & AI
Enterprise client Top 100
Technology & Consulting
250000 employees
No outsourcing - Kyndryl spin off 2021
Quantum development
Develop enterprise software solutions
Develop infrastructure
Software acquisitions

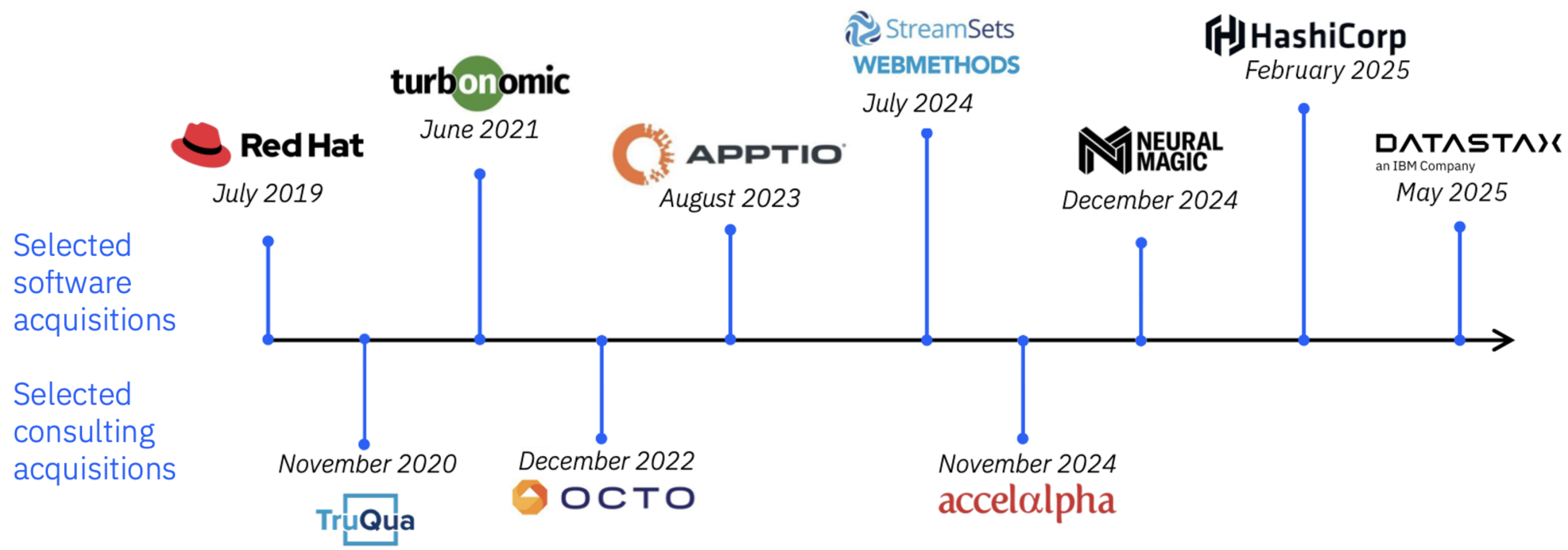
IBM's Integrated Portfolio



Consulting
Strategy and Technology ● Intelligent Operations
IBM Consulting Advantage
System Integrator Partners
Software
Automation ● Data ● Hybrid Cloud ● Transaction Processing
Software and SaaS Partners
watsonx .ai • .data • .governance • Orchestrate
Red Hat OpenShift • Enterprise Linux • Ansible
Infrastructure
IBM Z ● Distributed Hybrid Infrastructure ● Infrastructure Support
Public Clouds
AWS ● Azure ● Others
Enterprise Infrastructure
Edge

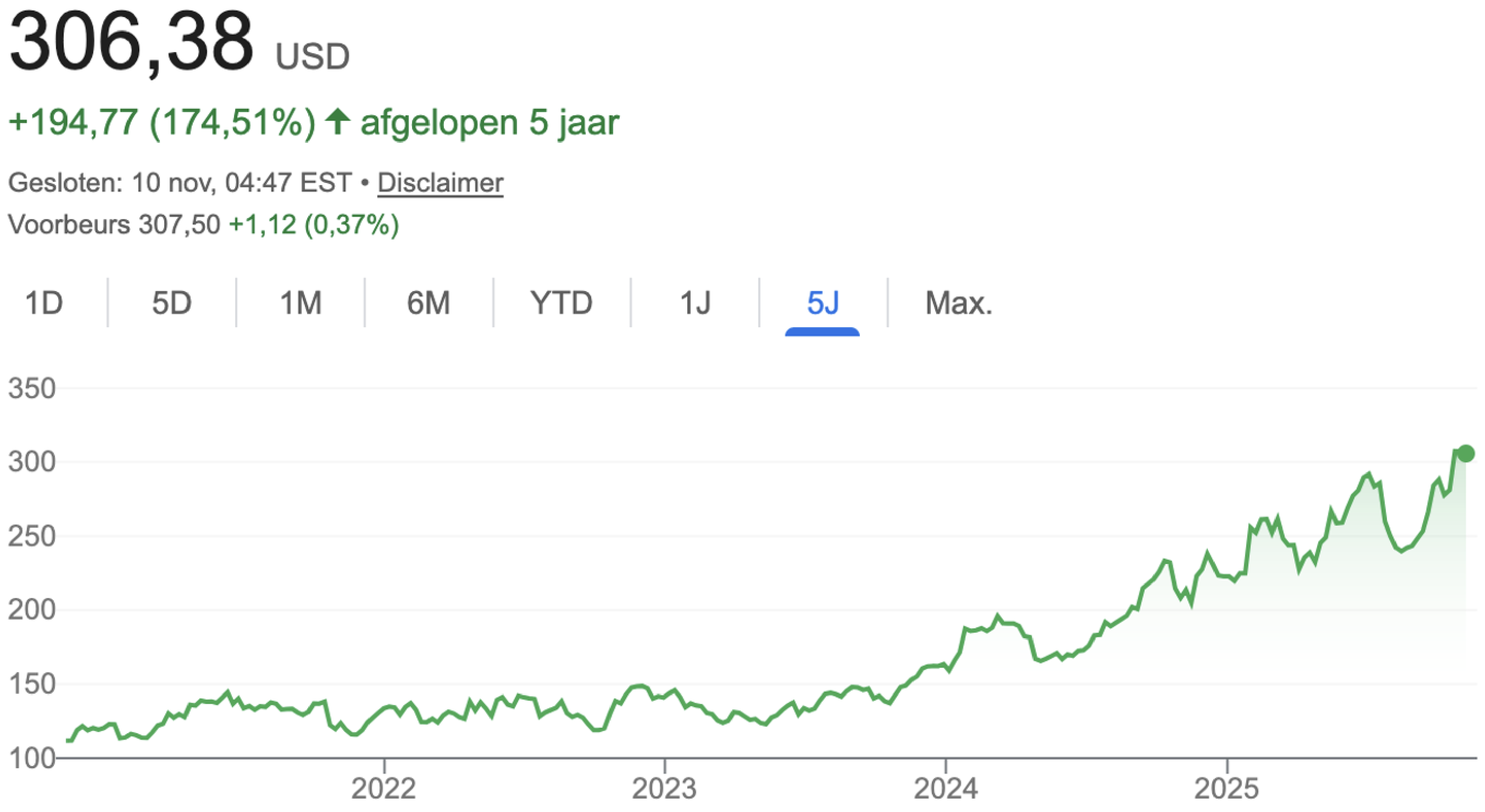
IBM Innovation | Augmented focus on acquisition strategy

75% of acquisition spent on Software



IBM share evolution

Hybrid cloud and AI impact


306,38 USD

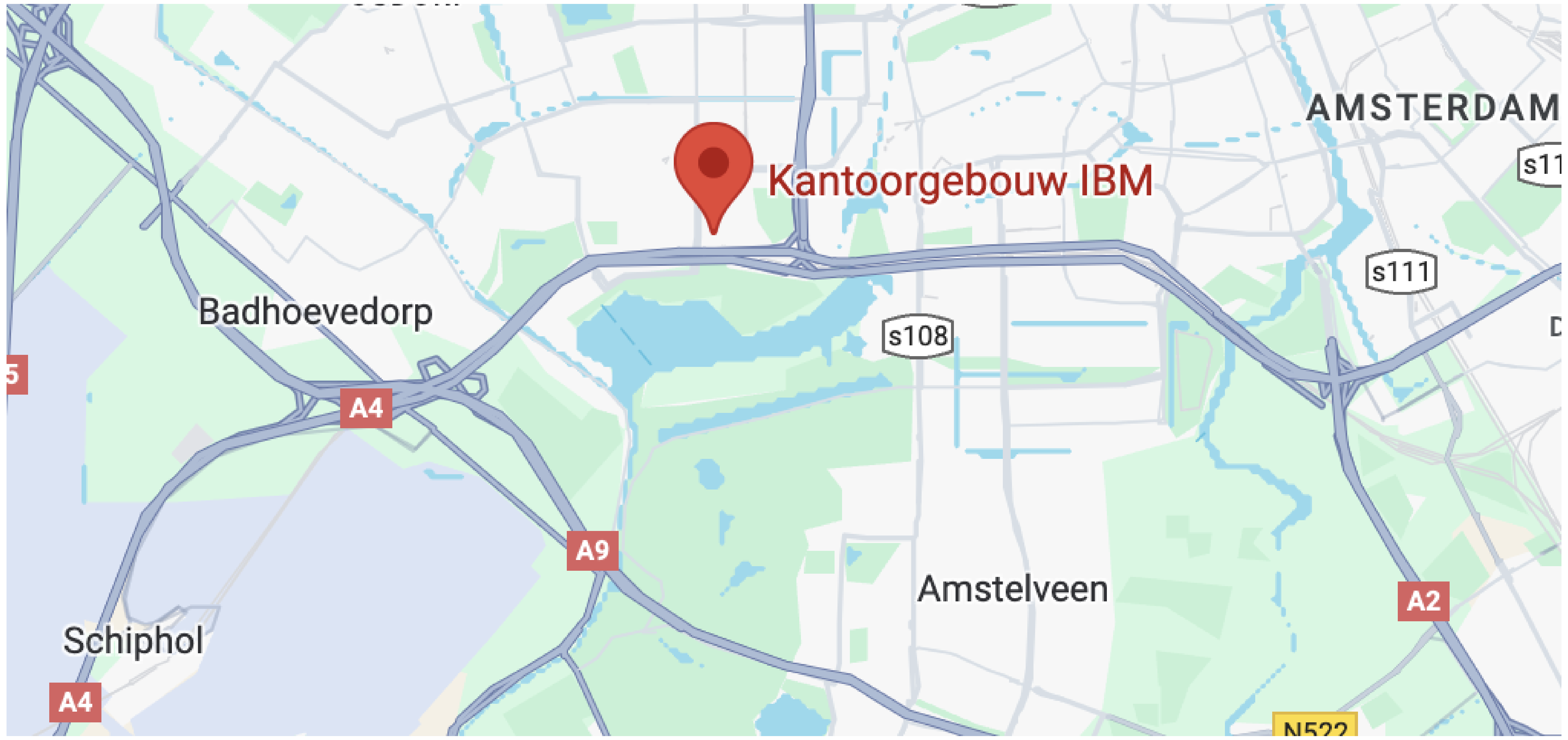
+194,77 (174,51%) ↑ afgelopen 5 jaar

Gesloten: 10 nov, 04:47 EST • Disclaimer

Voorbeurs 307,50 +1,12 (0,37%)

IBM The Netherlands in a glance

2028



Johan Huizingalaan 765
1200 Employees

Data & AI
Automation
Cloud
Security
Infrastructure
Services & Support

RIP

Why IBM Z?

Mission critical business transactions run on IBM Z®

>70%

of the world’s transactions run on the mainframe.*

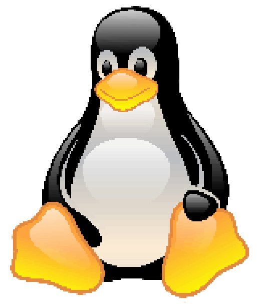
(IBM Z = Mainframe)

* Katov PhD, N. (April 2025), Mitigating Fraud in The AI Age: Supporting Transaction Fraud Detection at Scale on IBM z17, Celent
https://community.ibm.com/community/user/blogs/sarah-bowden/2025/05/15/ai-on-the-mainframe-how-the-ibm-z17-transforms-fra

Why IBM Z?

- ✓Security
- ✓Resiliency
- ✓Scalability
- ✓Performance
- ✓Availability

IBM LinuxONE



2000

Linux® for s390x

Red Hat® Enterprise Linux®

SUSE

Data serving (Oracle, Db2®)

2015

IBM® LinuxONE

Ubuntu

Data serving (MongoDB)

2018

IBM® LinuxONE II

IBM Db2® Analytics Accelerator

Core banking (Temenos)

2019

IBM® LinuxONE III

Secure execution

Digital assets (Metaco)

Red Hat® OpenShift® Container Platform

2022

IBM® LinuxONE 4

Quantum-safe encryption

Sustainability

Red Hat OpenShift Ansible® Automation Platform

Data serving (Fujitsu, EDB)

Core banking (Finacle)

2025

IBM® LinuxONE 5

Cost efficiency

Scalable AI

Confidential Containers (Red Hat OpenShift CoCo

Red Hat OpenShift Virtualization- technology preview

Red Hat OpenShift AI- technology preview

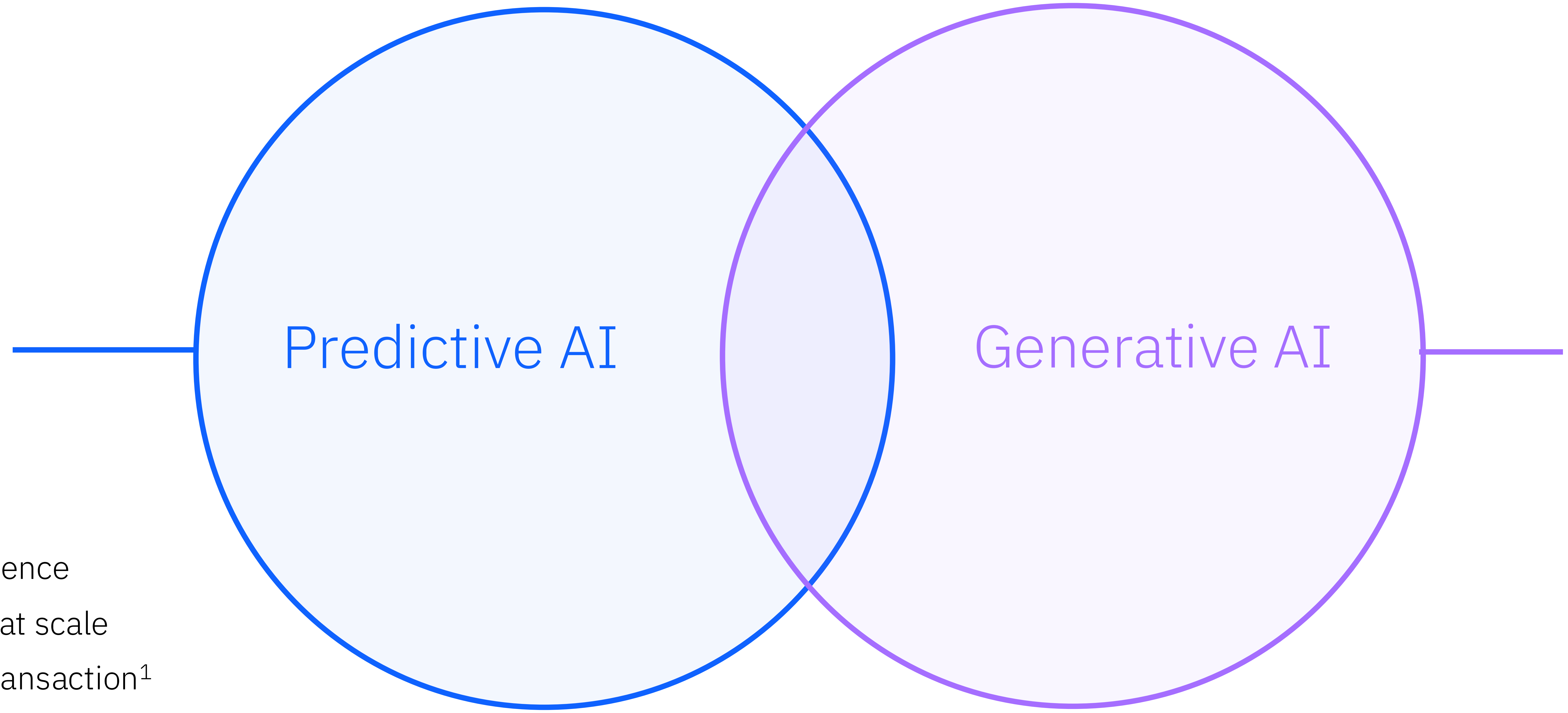
HashiCorp integration

Predictive AI and generative AI on IBM z17 deliver unique capabilities

Machine learning

Advantage

- Real-time AI inference
- In-transaction AI at scale
- Inference every transaction[1]



Larger, more complex models

Advantage

- Gen AI with IBM Z RAS
- Security and data protection
- Energy efficiency

Multiple-model AI at speed and scale

Combine machine learning
and LLMs to achieve higher prediction accuracy
and expanded insights

AI on IBM Z: make more valuable outcomes possible for every industry

Financial Services

- FRAUD DETECTION
- ANTI-MONEY LAUNDERING
- RISK SCORING
- CREDIT DECISIONING

Insurance

- CLAIMS FRAUD DETECTION
- INTELLIGENT UNDERWRITING
- TEXT/IMAGE PROCESSING
- PRODUCT RECOMMENDATIONS

Government

- GEOSPATIAL IMAGE ANALYSIS
- FRAUD & SENTIMENT ANALYSIS
- AUDIT & COMPLIANCE
- CHAT SERVICE

Others

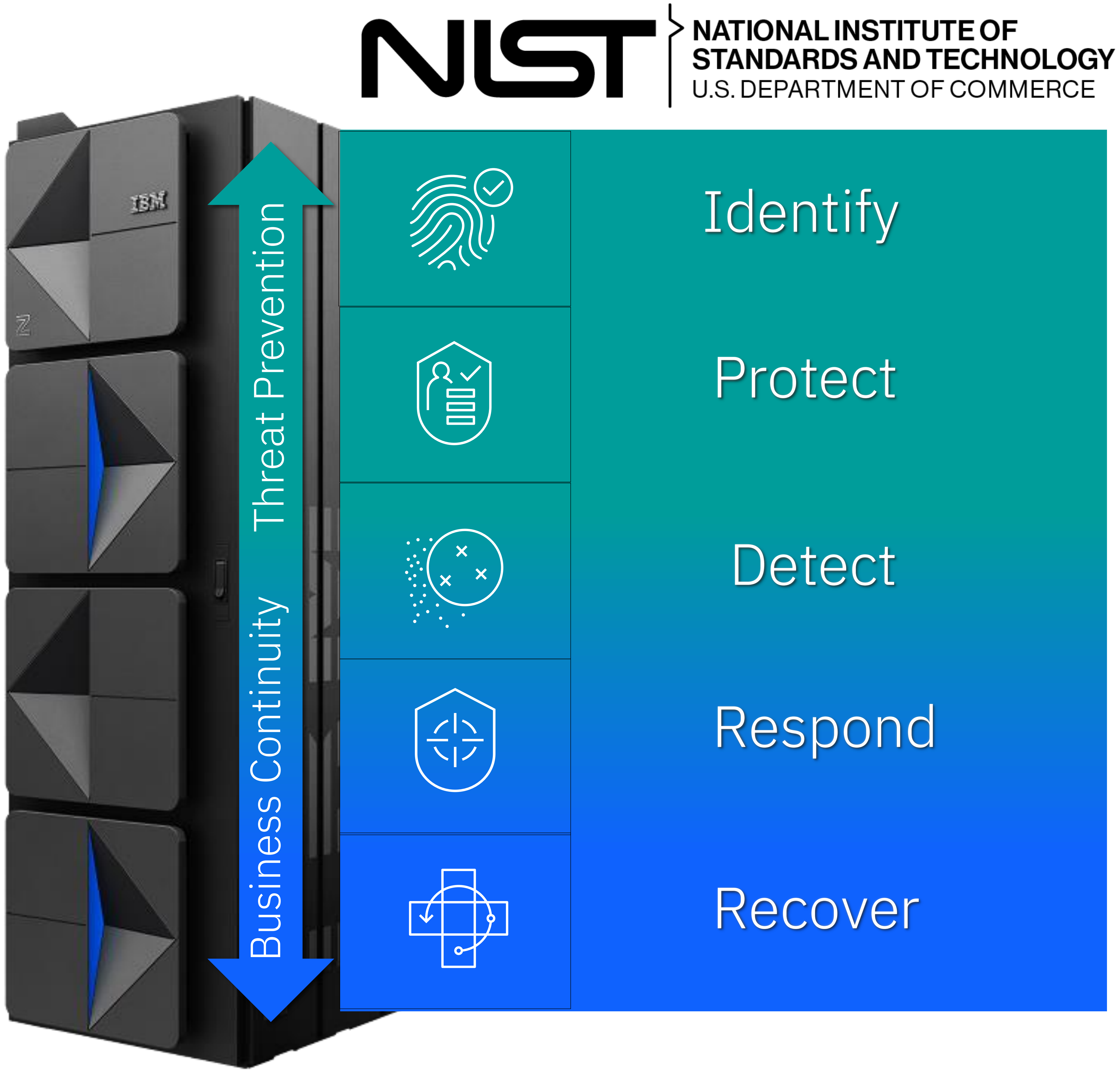
- RETAIL INVENTORY/DEMAND FORECASTING
- SYSTEM ADMIN ASSISTANT
- CODE ASSISTANT
- TRANSPORTATION LOGISTICS

A comprehensive security strategy for IBM Z

Addressing threat *prevention* and business continuity needs tailored to your environment.

Comprehensive in scope to enable an organization to demonstrate *compliance* with the specific standards and regulations relevant to its industry.

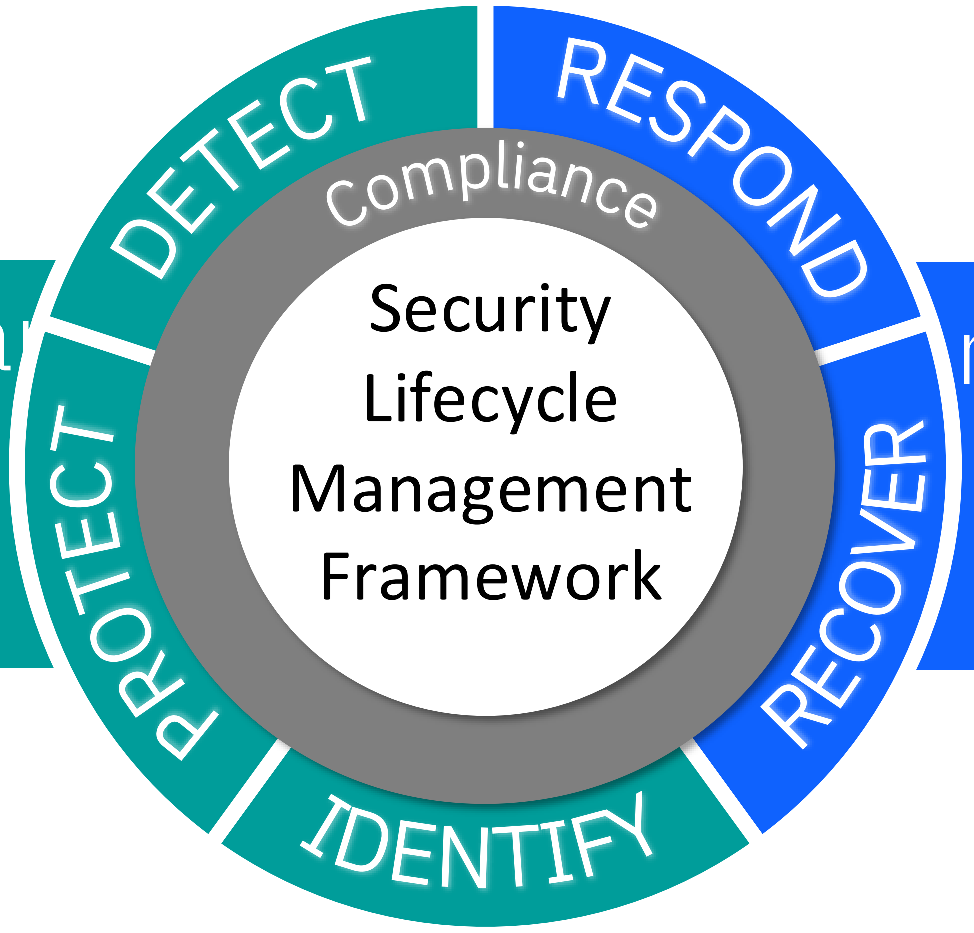
Utilizes the [NIST Cybersecurity framework]



Comprehensive full stack security and resiliency strategy

Cyber Security

Focused on **prevention**, aiming to safeguard a
environment from unauthorized
access and malicious activities



Cyber Resiliency

n organization's ability to swiftly **respond** and
resume operations in the event
of a cyber-incident

DISA

PCI DSS COMPLIANT

DORA Digital Operational Resilience Act

CIS. Center for Internet Security®

IBM Z® Unique Capabilities

AI-powered innovation

- Continuous threat and vulnerability management
- Network segmentation and system hardening
- AI powered classification of data

Reliable & Secure System

- z/OS® Statement of Integrity
- Pervasive Encryption
- Secure Boot
- Quantum Safe
- Crypto Accelerator
- Secure Execution for Linux
- GDPS® & LCP
- Cyber Vault

Automated for Efficiency

- IBM Z Compliance Center
- Crypto Discovery and Inventory
- IBM Concert

EU timeline for the transition to Post-Quantum Cryptography

By 31.12.2026:

- At least the First Steps have been implemented by all Member States.
- Initial national PQC transition roadmaps have been established by all Member States.
- PQC transition planning and pilots for high- and medium-risk use cases have been initiated.

By 31.12.2030:

- The Next Steps have been implemented by all Member States.
- The PQC transition for high-risk use cases has been completed.
- PQC transition planning and pilots for medium-risk use cases have been completed.
- Quantum-safe software and firmware upgrades are enabled by default.

By 31.12.2035:

- The PQC transition for medium-risk use cases has been completed.
- The PQC transition for low-risk use cases has been completed as much as feasible.

Source: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

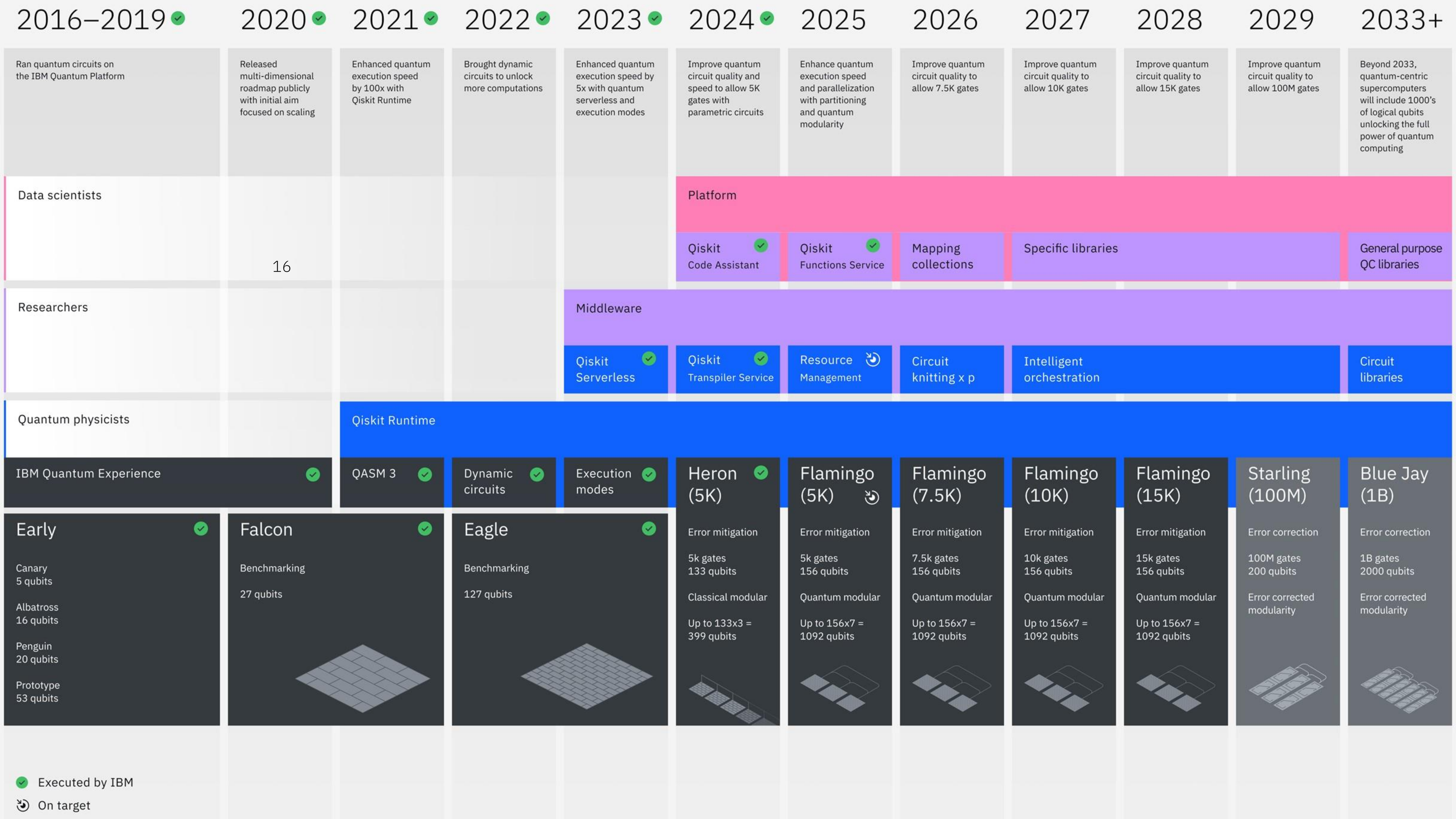
Updated IBM development roadmap

Our updated development roadmap charts our course for delivering client-facing systems and services. It now focuses both on qubit count and on the size of the circuits that our systems can run, tracked by the number of gates
in those circuits.

You can start exploring quantum utility today, and this roadmap shows how the quantum workload size available for that exploration will increase.

Our challenge is to develop the tools that users need to explore quantum utility and unlock the full power of quantum-centric supercomputing by 2033.

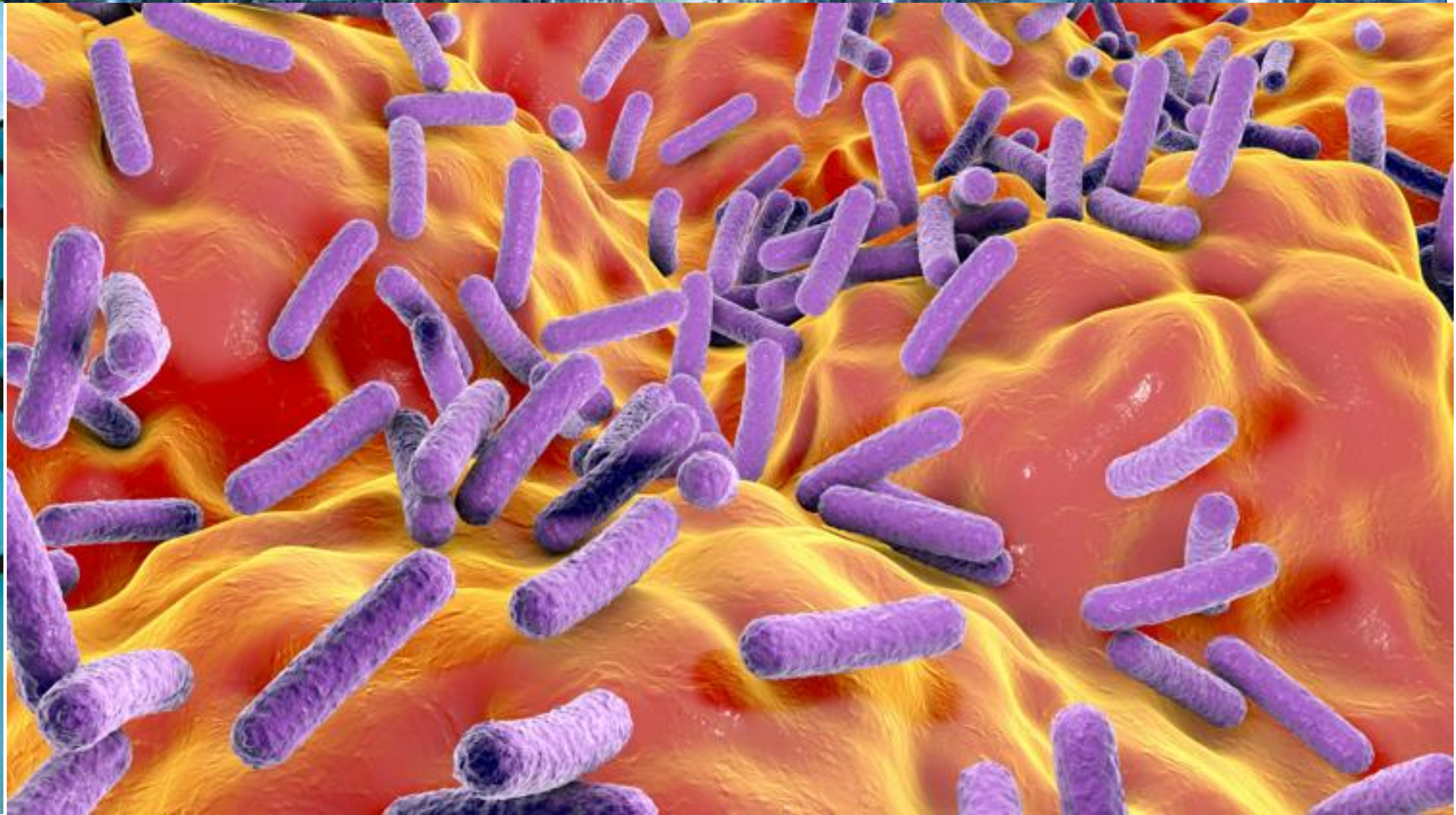
We will also incorporate advances in machine learning and generative AI to turbocharge our software's performance.



	2016–2019 ✓	2020 ✓	2021 ✓	2022 ✓	2023 ✓	2024 ✓	2025	2026	2027	2028	2029	2033+
	Ran quantum circuits on the IBM Quantum Platform	Released multi-dimensional roadmap publicly with initial aim focused on scaling	Enhanced quantum execution speed by 100x with Qiskit Runtime	Brought dynamic circuits to unlock more computations	Enhanced quantum execution speed by 5x with quantum serverless and execution modes	Improve quantum circuit quality and speed to allow 5K gates with parametric circuits	Enhance quantum execution speed and parallelization with partitioning and quantum modularity	Improve quantum circuit quality to allow 7.5K gates	Improve quantum circuit quality to allow 10K gates	Improve quantum circuit quality to allow 15K gates	Improve quantum circuit quality to allow 100M gates	Beyond 2033, quantum-centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing
Data scientists		16				Platform Qiskit ✓ Code Assistant	Qiskit ✓ Functions Service	Mapping collections	Specific libraries			General purpose QC libraries
Researchers					Middleware Qiskit ✓ Serverless	Qiskit ✓ Transpiler Service	Resource ◔ Management	Circuit knitting x p	Intelligent orchestration			Circuit libraries
Quantum physicists			Qiskit Runtime									
	IBM Quantum Experience ✓		QASM 3 ✓	Dynamic circuits ✓	Execution modes ✓	Heron (5K) ✓ Error mitigation 5k gates 133 qubits Classical modular Up to 133x3 = 399 qubits	Flamingo (5K) ◔ Error mitigation 5k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Flamingo (7.5K) Error mitigation 7.5k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Flamingo (10K) Error mitigation 10k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Flamingo (15K) Error mitigation 15k gates 156 qubits Quantum modular Up to 156x7 = 1092 qubits	Starling (100M) Error correction 100M gates 200 qubits Error corrected modularity	Blue Jay (1B) Error correction 1B gates 2000 qubits Error corrected modularity
	Early ✓ Canary 5 qubits Albatross 16 qubits Penguin 20 qubits Prototype 53 qubits	Falcon ✓ Benchmarking 27 qubits		Eagle ✓ Benchmarking 127 qubits								

✓ Executed by IBM
◔ On target

C-2301



We are entering a new cryptographic era

Harvest now,
decrypt later

Availability of “cryptographically relevant” quantum computers

Before

After

Harvest confidential data to decrypt 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 modern digital world depends on cryptography

And quantum computing is ushering in a new cryptographic era

Prime factors

= p x q

For RSA

2048-bit composite integer

25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357

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

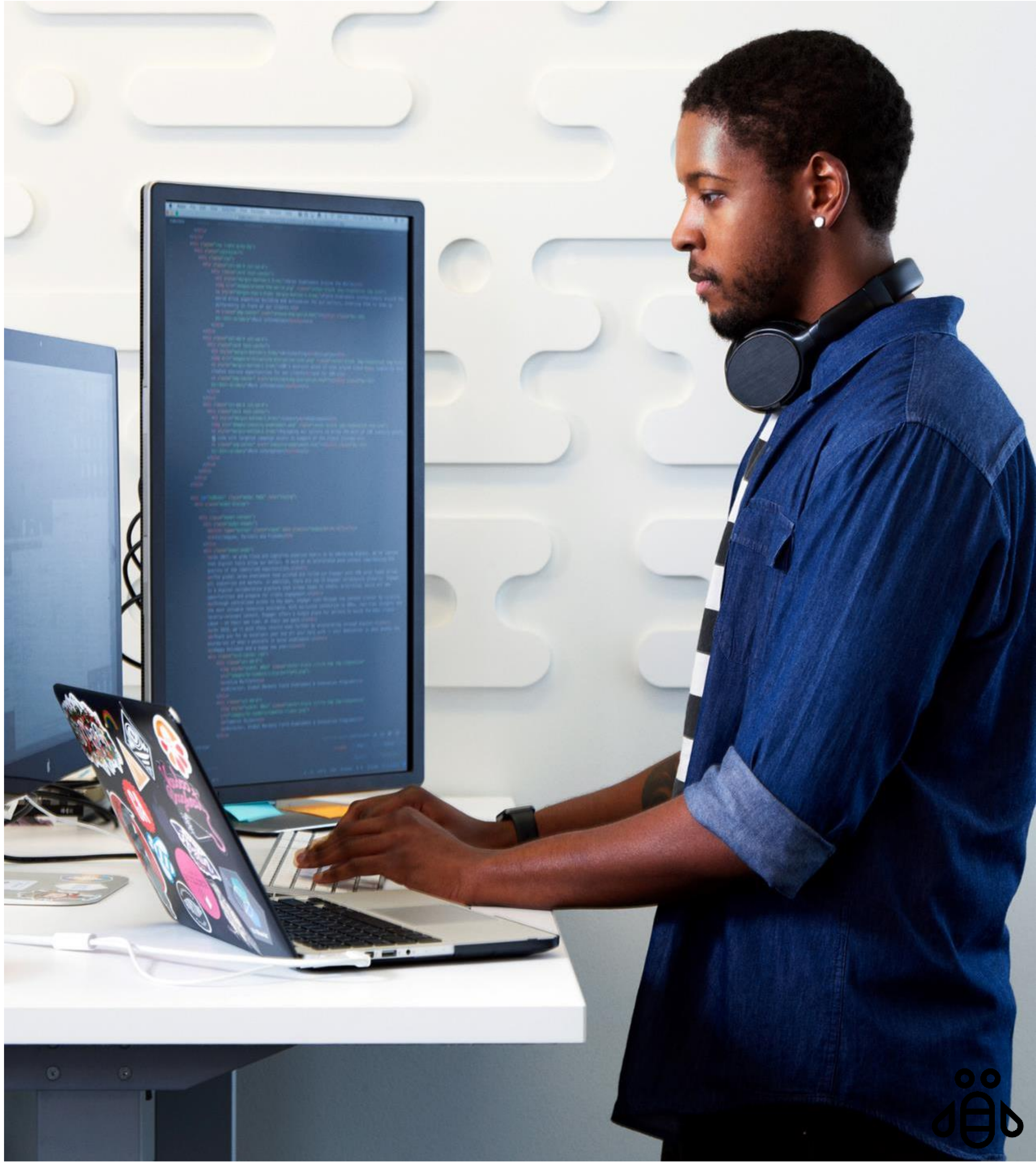
We need quantum-safe cryptography …

Quantum-safe cryptography refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built.

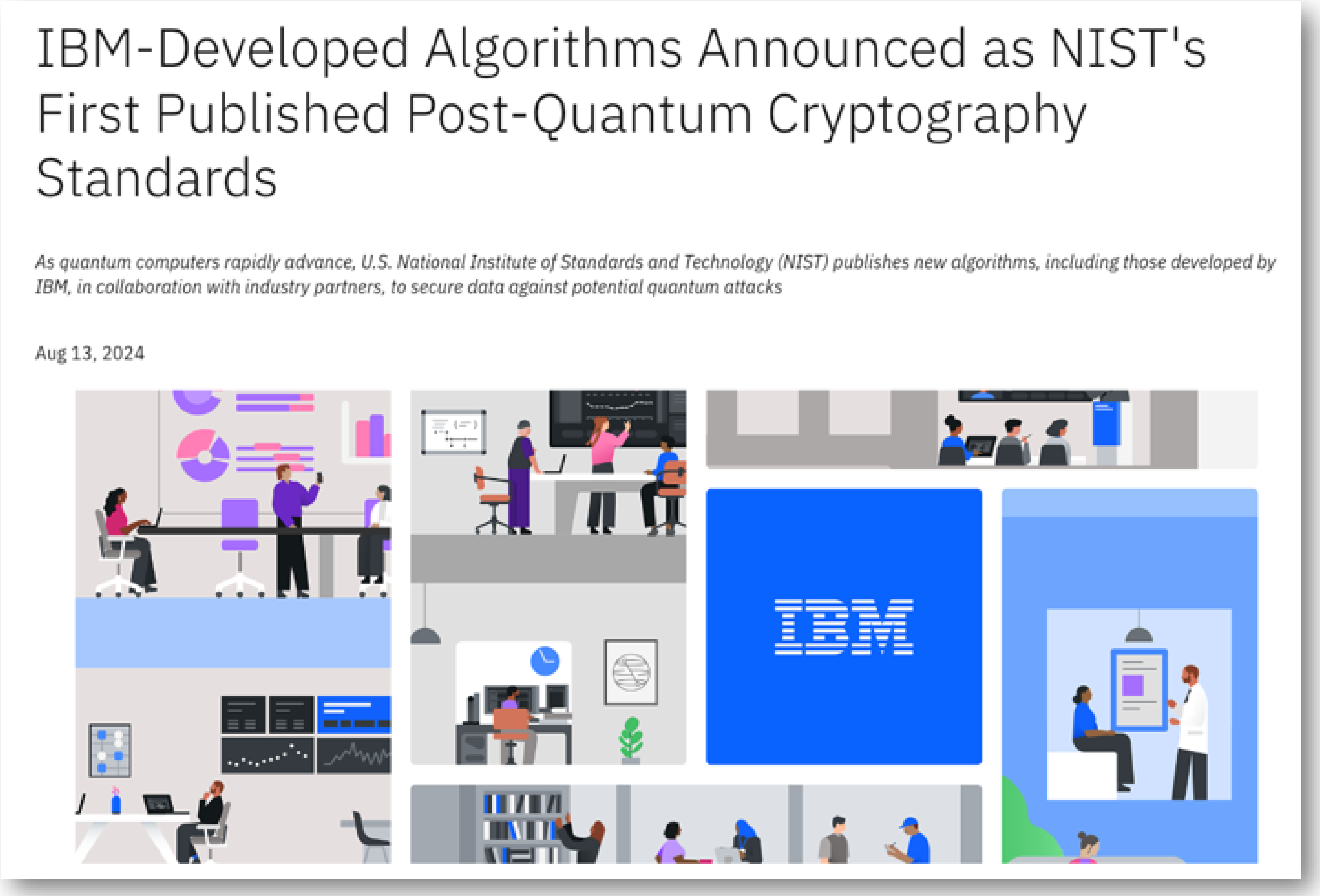
The Wait is Over!

On August 13, 2024, the US National Institute of Standards and Technology published the first set of quantum safe algorithms.

Source: https://www.etsi.org/technologies/quantum-safe-cryptography



NIST PQC Standards



IBM-Developed Algorithms Announced as NIST's First Published Post-Quantum Cryptography Standards

As quantum computers rapidly advance, U.S. National Institute of Standards and Technology (NIST) publishes new algorithms, including those developed by IBM, in collaboration with industry partners, to secure data against potential quantum attacks

Aug 13, 2024

ML-Kem FIPS 203

F.K.A CRYSTALS-Kyber

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

ML-DSS FIPS 204

F.K.A. CRYSTALS-Dilithium

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

SLH-DSA FIPS 205

F.K.A. SPHINCS^{+}

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

FN-DSA FIPS 206

F.K.A. Falcon

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

Rebuild the cryptographic solutions

Quantum-safe cryptography/Post-quantum cryptography (PQC)

New lattice-based cryptography

Resistant to classical and quantum attacks

Runs on classical computers!

NIST process

Standardization of PQC for key encapsulation and digital signature started in 2016

Standards (FIPS 203, FIPS 204, FIPS 205) published Aug 2024

On-going cryptography standardization program

(IBM Research Zurich)

Cryptographic protocols

Major cryptographic protocols, such as TLS and IPSec need to be adapted in order to use quantum-safe algorithms

Related activities to update or create new RFCs are ongoing at the IETF

Migration

The migration to Quantum-safe affects the entire IT estate:

- Software development
- Vendor products
- Software as a service
- Infrastructure, network, devices, etc.

and needs new capabilities such as cryptographic discovery & cryptographic agility

Quantum-safe is NOT just about the data

Ensure that the system (i.e. firmware, OS, VM, container, application) has not been hacked, altered, updated, damaged, or modified in any way
since it was created by the manufacturer, installed, and/or started

IBM Z and IBM LinuxONE

→ ## End-to-end cybersecurity and privacy

- Deploy confidential containers, built to protect your data and applications.
- Address quantum-enabled cybersecurity risks with pioneering quantum-safe encryption from IBM.
- Scale and unify your encryption across the enterprise.

Security built into every layer of the stack for end-to-end secured computing solutions

→ FIPS level 140-2 L4 hardware security modules

→ Confidential computing

→ Quantum-safe secure boot and crypto APIs

→ Hardware protected keys

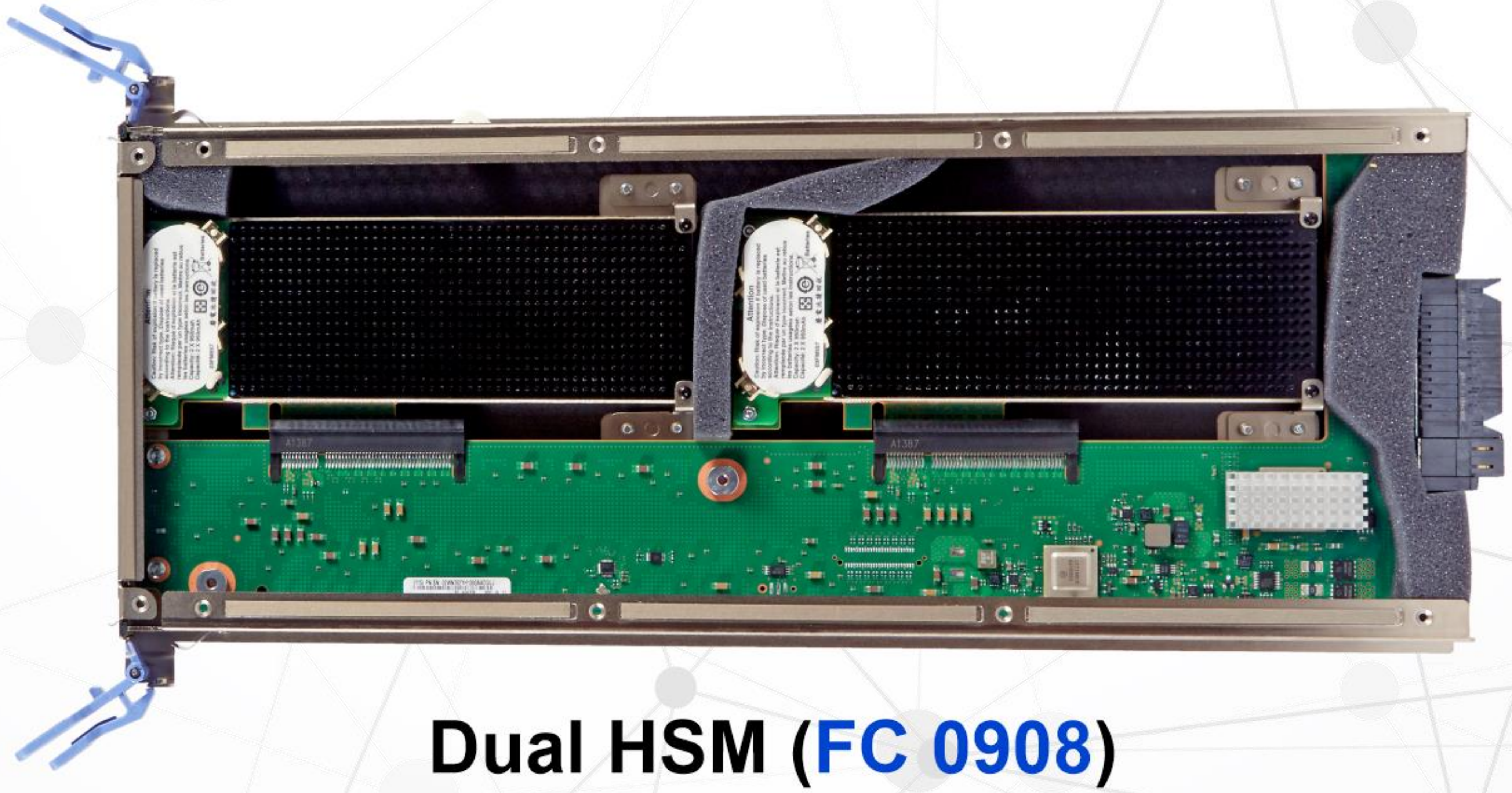
→ Dual HW accelerated cryptography

→ Common criteria isolation (LPAR)

Crypto Express8S HSM
(IBM 4770 Cryptographic Hardware Security Module)

- Preprocessing and functionality offloaded from the main processor unit
- Provides hardware acceleration of Dilithium and Kyber algorithms for quantum-safe support
- Supports hybrid cryptographic schemes leveraging classical and quantum-safe cryptographic algorithms
- Designed to be **FIPS 140-2 Level 4** compliant
- Three configuration modes:
  - Common Cryptographic Architecture (CCA)
  - Enterprise Public Key Cryptography Standards #11 (EP11)
  - Accelerator

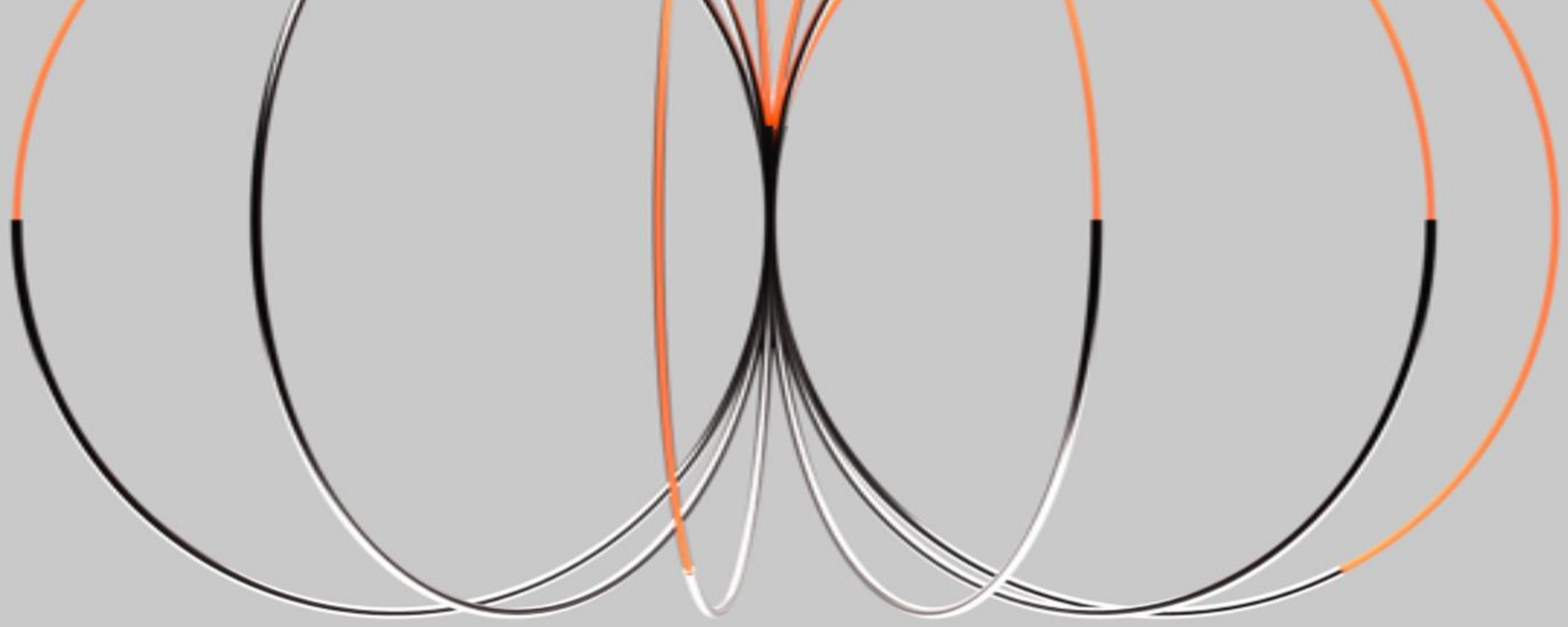
Quantum-safe algorithm (QSA) support, adding CRYSTALS-Dilithium Round 3 keys, as well as hardware support for Dilithium keys. In addition, for QSA, CRYSTALS-Kyber keys for encryption and key exchange are supported.



Dual HSM (FC 0908)

Secure your data and applications with confidential computing

Confidential computing with integrated acceleration for AI, post-quantum encryption and data compression

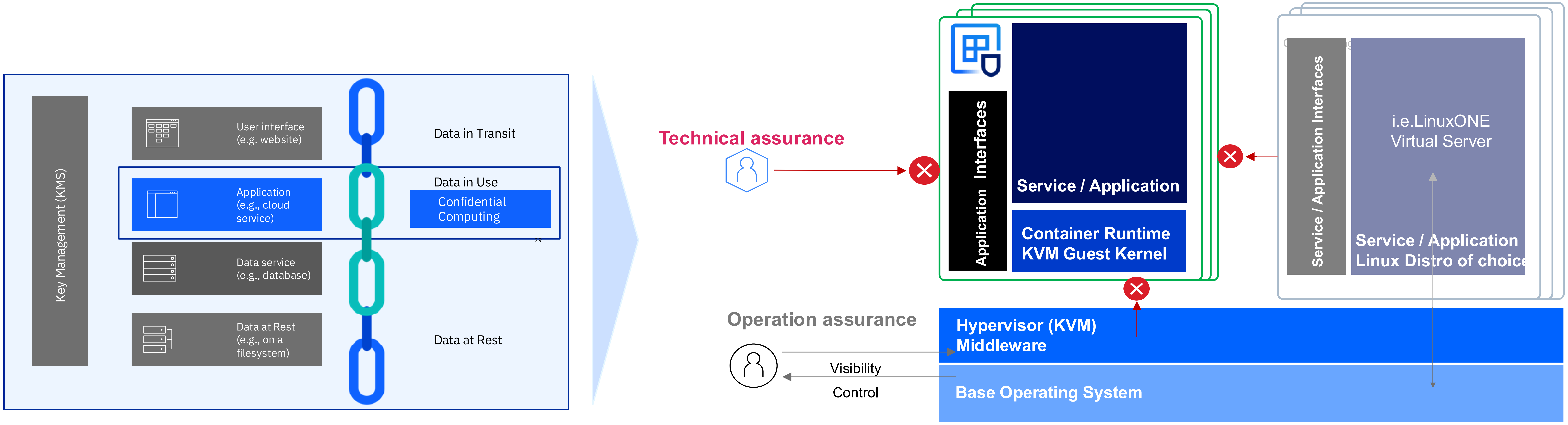


Leverage confidential computing to protect AI models, data and applications for collaborative learning and inference

Turnkey data sovereignty and separation of duty that does not depend on third parties to authenticate

Unique capabilities: integrated acceleration and key management to enforce policies with a zero-trust approach

Hyper Protect Virtual Servers based on Secure Execution for Linux



Enhanced protection boundary

Isolation between instances

Isolation from the OS and Hypervisor vulnerabilities

Zero Trust principles based on an encrypted contract concept. Multiple personas can collaborate without data compromise, deployment can be validated by auditor persona

Malware protection with Secure Build to ensure that only authorized code can run

Technical assurance

Data can’t be accessed by unauthorized party or admin

Highlights of security solutions available on IBM Z and IBM LinuxONE

- Unified Key Orchestrator
- IBM Vault
- Guardium Key Lifecycle Manager
- Advanced Crypto Service Provider

Key management is vital to encryption, but challenging

Reasons that can make key management painful

- Unclear ownership of the key management function
- Lack of technical expertise and skilled resources
- Isolated or fragmented key management systems
- Operational complexity
- Compliance with ever-evolving regulations and policies

Sources:
Ponemon Institute’s 2024 State of Zero Trust & Encryption Study
Encryption Consulting’s Study on Global Encryption Trends – 2024

Bring Your Own Key vs **Keep Your Own Key**

Giving customers exclusive control over their encryption keys. Only authorized users have access-no privileged users, including IBM Cloud admins, have access. IBM is the only cloud vendor to offer Keep Your Own Key - all other cloud providers offer Bring Your Own Key, where the customers generate the keys and provide them to the cloud service provider (CSP). This provides operational assurance which says the CSP will not access the keys. KYOK offers technical assurance where the cloud service provider *cannot* access the keys.

Data protection = Key protection

Sensitive

Confidential

Internal

Public

Increasing sensitivity requires increasing Control

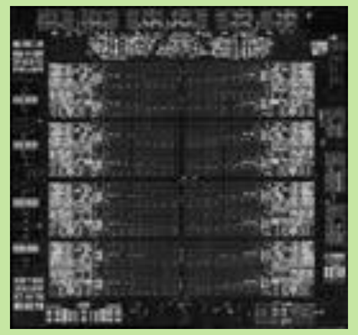
High security

Secure Key

Key values are encrypted under a Master Key. Crypto operations are performed only on a Hardware Security Module

Speed & Security Hybrid

Protected Key



Key values are encrypted under a wrapping key. Crypto operations are performed only using dedicated on-chip hardware

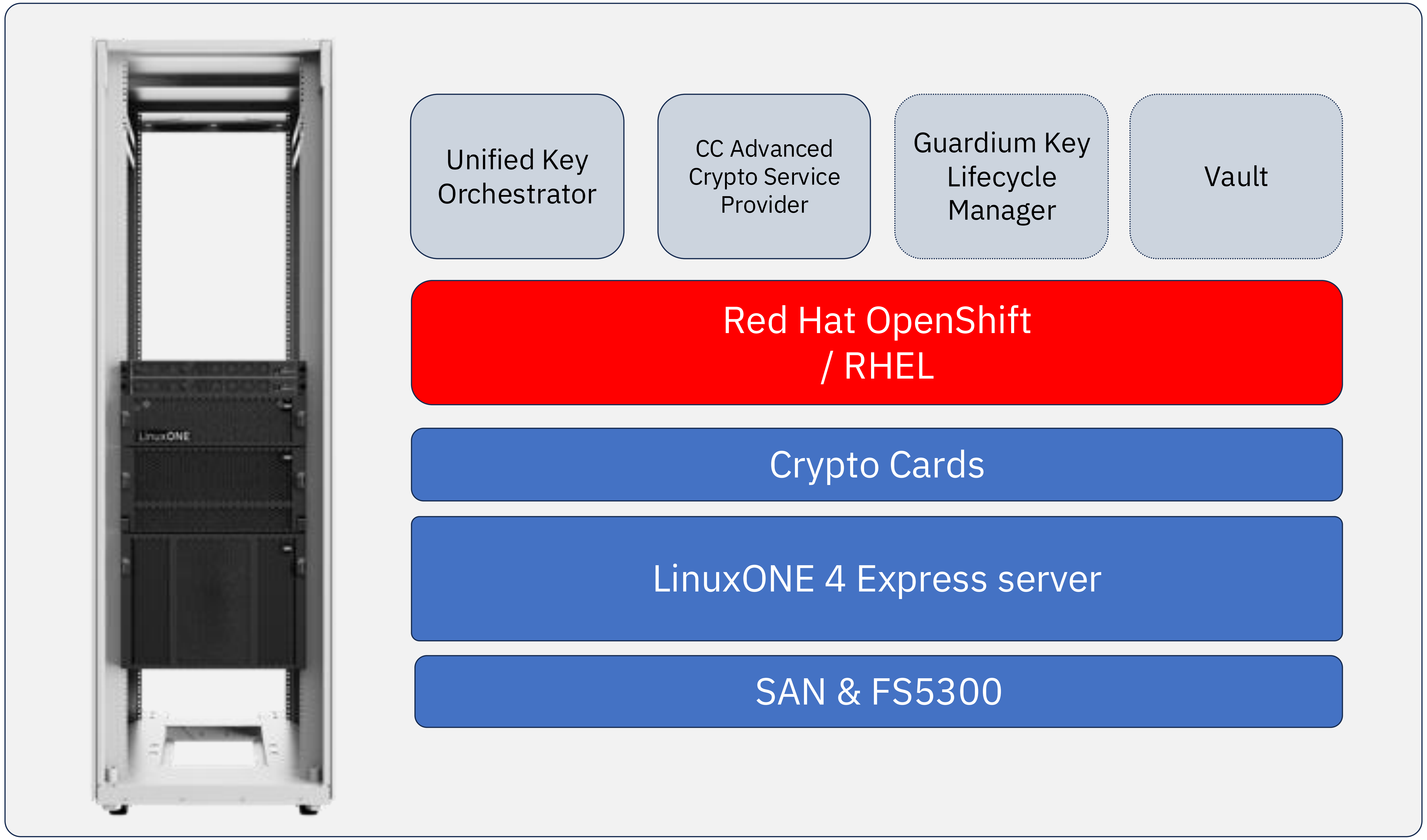
High speed

Clear Key

Key values are not encrypted. Crypto operations are performed outside of TEE

Post-Quantum Security Nerve Center

You don’t need to wait – you can start today November 20th, 2025



Unified Key Orchestrator

CC Advanced Crypto Service Provider

Guardium Key Lifecycle Manager

Vault

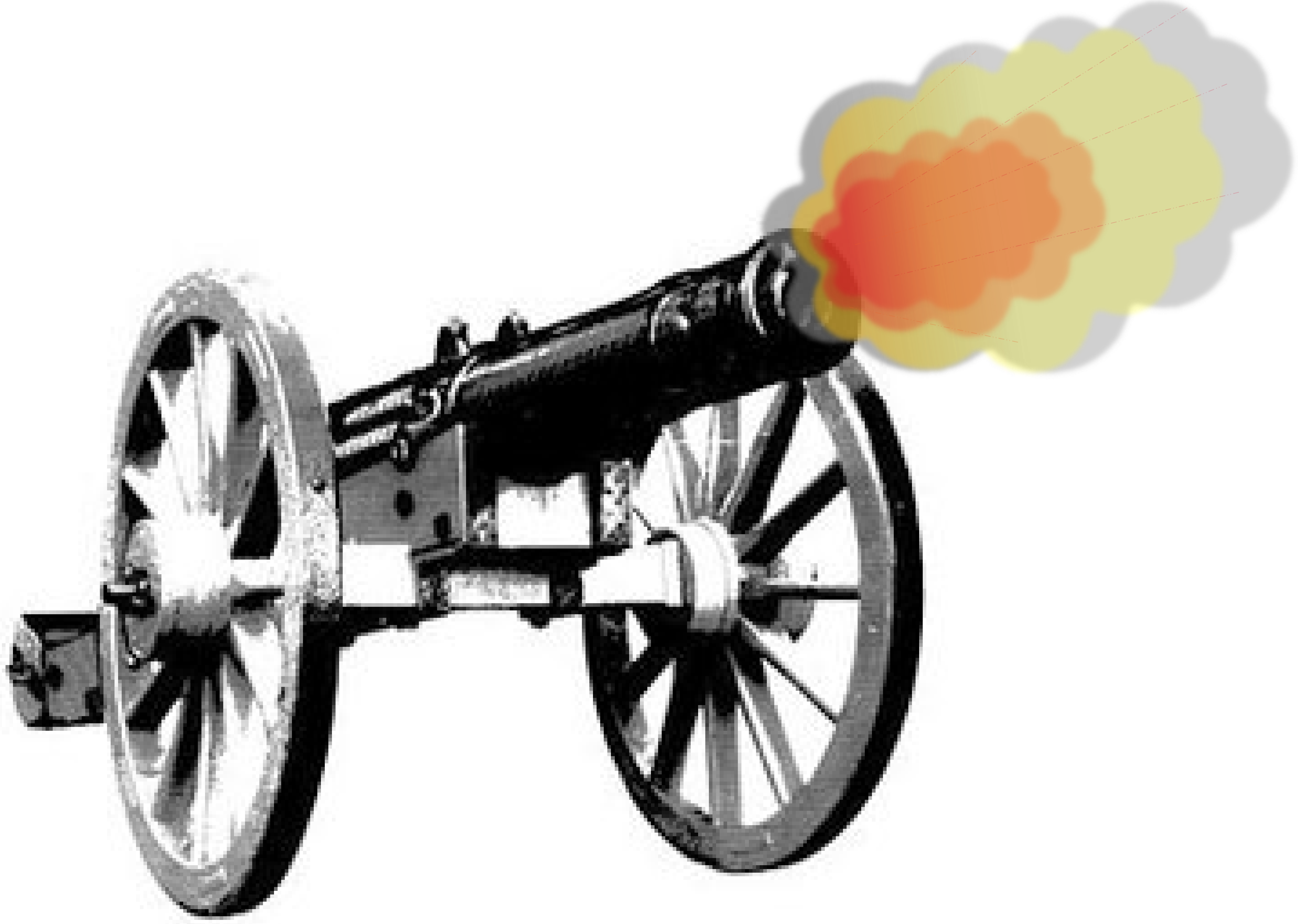
Red Hat OpenShift / RHEL

Crypto Cards

LinuxONE 4 Express server

SAN & FS5300

We Salute You



thatfinnishguy@fi.ibm.com

-
-
-
-
- IBM Spyre Accelerator is in tech preview until Q42025
- 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.
- Client examples are presented as illustrations of how those clients have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- 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.
- All names and references for organizations and other business institutions used in this deliverable’s scenarios are fictional. Any match with real organizations or institutions is coincidental.
- All names and associated information for people in this deliverable’s scenarios are fictional. Any match with a real person is coincidental. Videos may show information about or belonging to third parties. Such videos do not suggest endorsement of third parties or their products or services.