IBM

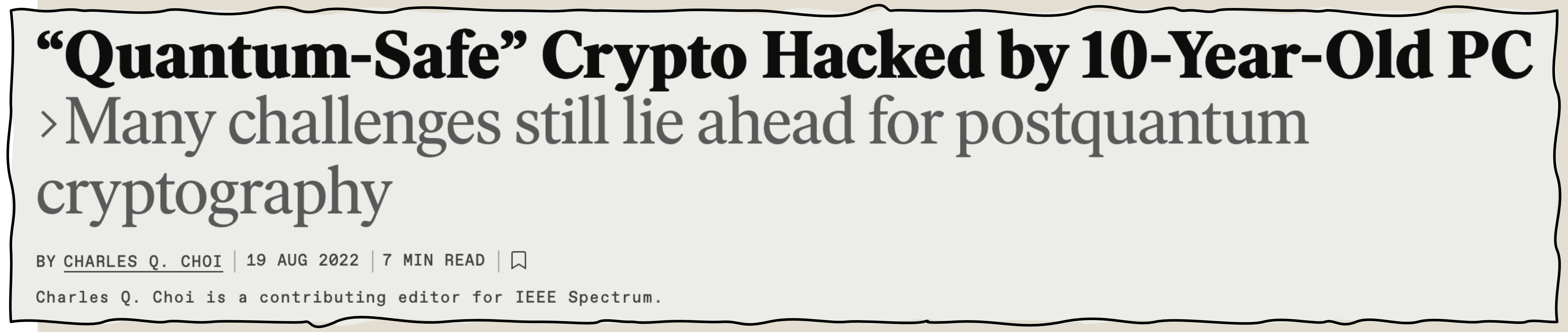
Pioneering Quantum Safety:

Securing Tomorrow’s Digital World

Agenda:

- **Securing the Quantum Future: A Leadership Imperative**
- **The Reality of Quantum Risk: What CISOs Need to Know**
- **How to Take Action Now**
- **Collaborating for Quantum-safe**

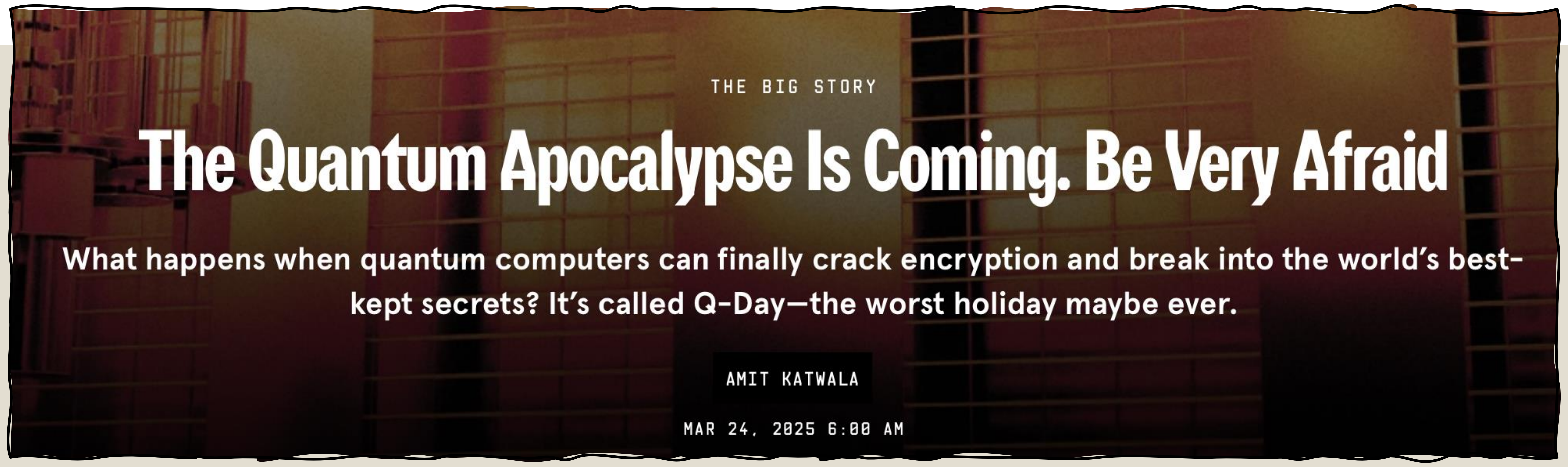
Urgency is in the air


“Quantum-Safe” Crypto Hacked by 10-Year-Old PC

› Many challenges still lie ahead for postquantum cryptography

BY CHARLES Q. CHOI | 19 AUG 2022 | 7 MIN READ

Charles Q. Choi is a contributing editor for IEEE Spectrum.


THE BIG STORY

The Quantum Apocalypse Is Coming. Be Very Afraid

What happens when quantum computers can finally crack encryption and break into the world’s best-kept secrets? It’s called Q-Day—the worst holiday maybe ever.

AMIT KATWALA

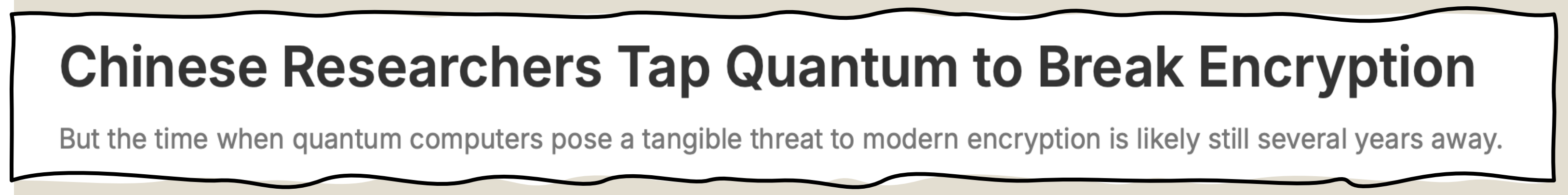
MAR 24, 2025 6:00 AM

The Next Big Cyber Threat Could Come from Quantum Computers… Is the Government Ready?

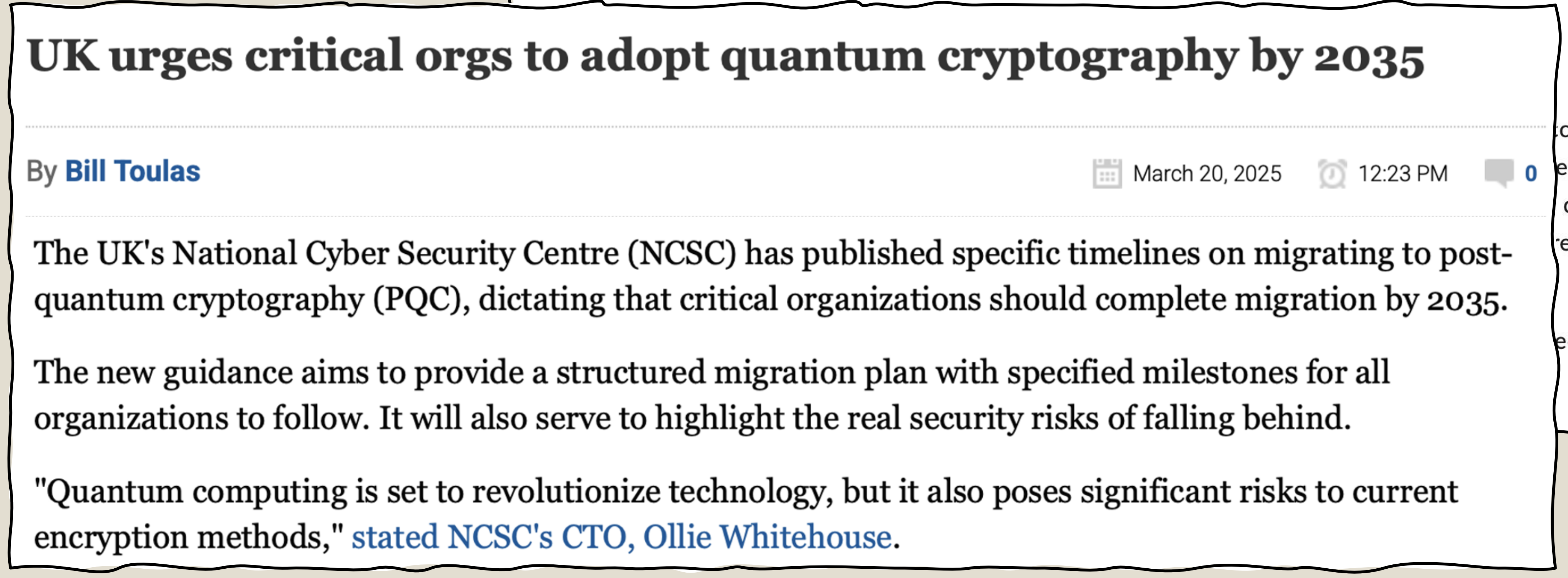
Posted on January 22, 2025

count—
erging
could also be
e like
ederal strategy

Related Posts


Chinese Researchers Tap Quantum to Break Encryption

But the time when quantum computers pose a tangible threat to modern encryption is likely still several years away.


UK urges critical orgs to adopt quantum cryptography by 2035

By Bill Toulas March 20, 2025 12:23 PM 0

The UK's National Cyber Security Centre (NCSC) has published specific timelines on migrating to post-quantum cryptography (PQC), dictating that critical organizations should complete migration by 2035.

The new guidance aims to provide a structured migration plan with specified milestones for all organizations to follow. It will also serve to highlight the real security risks of falling behind.

"Quantum computing is set to revolutionize technology, but it also poses significant risks to current encryption methods," stated NCSC's CTO, Ollie Whitehouse.

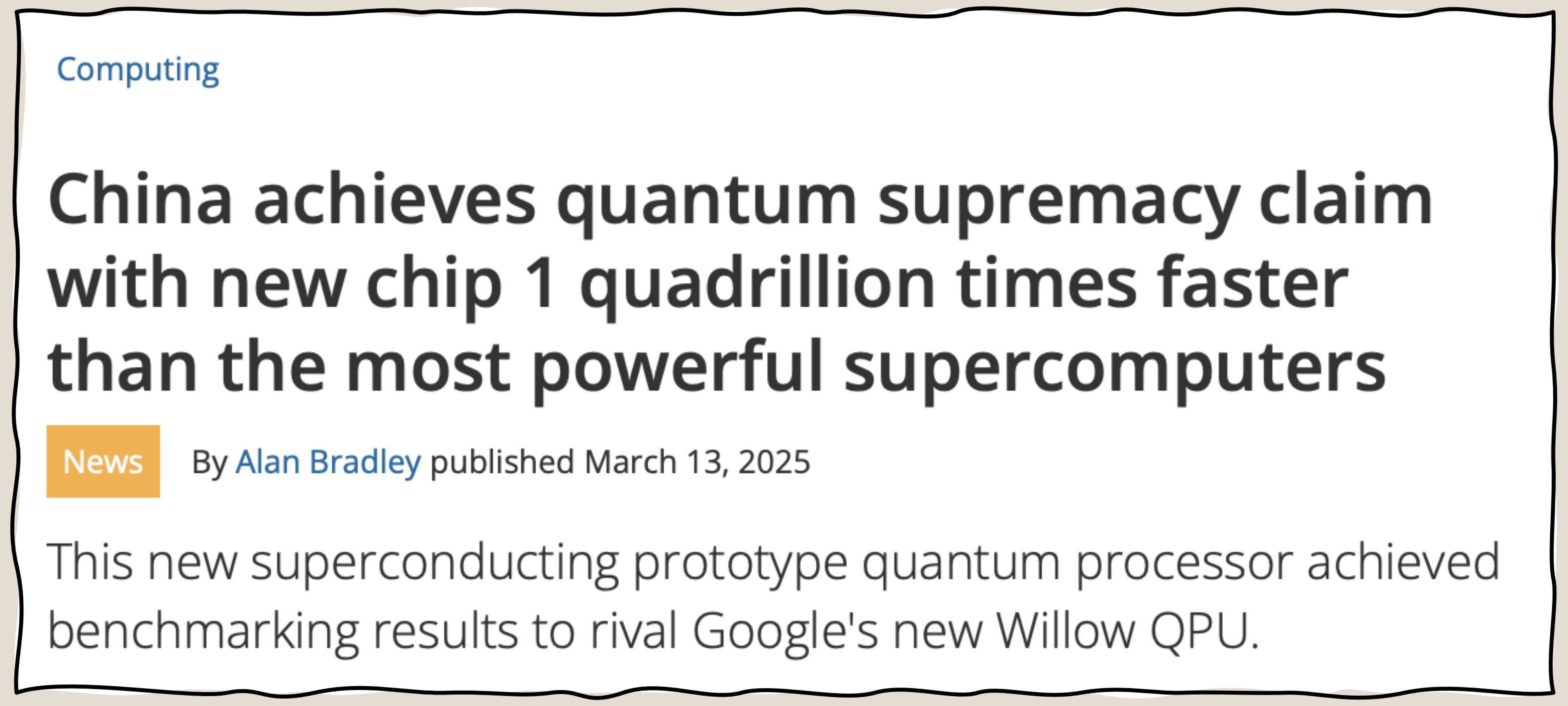
Preparing for the Quantum Threat: The Urgent Need for Next-Generation Cryptography

As quantum computing advances, organizations must adopt future-proof security strategies to safeguard data against emerging threats

Thomas Lintemuth, Distinguished VP analyst, Gartner
March 19, 2025

4 Min Read

Quantum Latest News


Computing

China achieves quantum supremacy claim with new chip 1 quadrillion times faster than the most powerful supercomputers

News By Alan Bradley published March 13, 2025

This new superconducting prototype quantum processor achieved benchmarking results to rival Google's new Willow QPU.

Quantum computing is coming for your cryptography, warns NCSC

No need to panic just yet, but plans to move to quantum-safe alternatives should be in place by 2028 at the latest

John Leonard
20 March 2025 • 3 min read

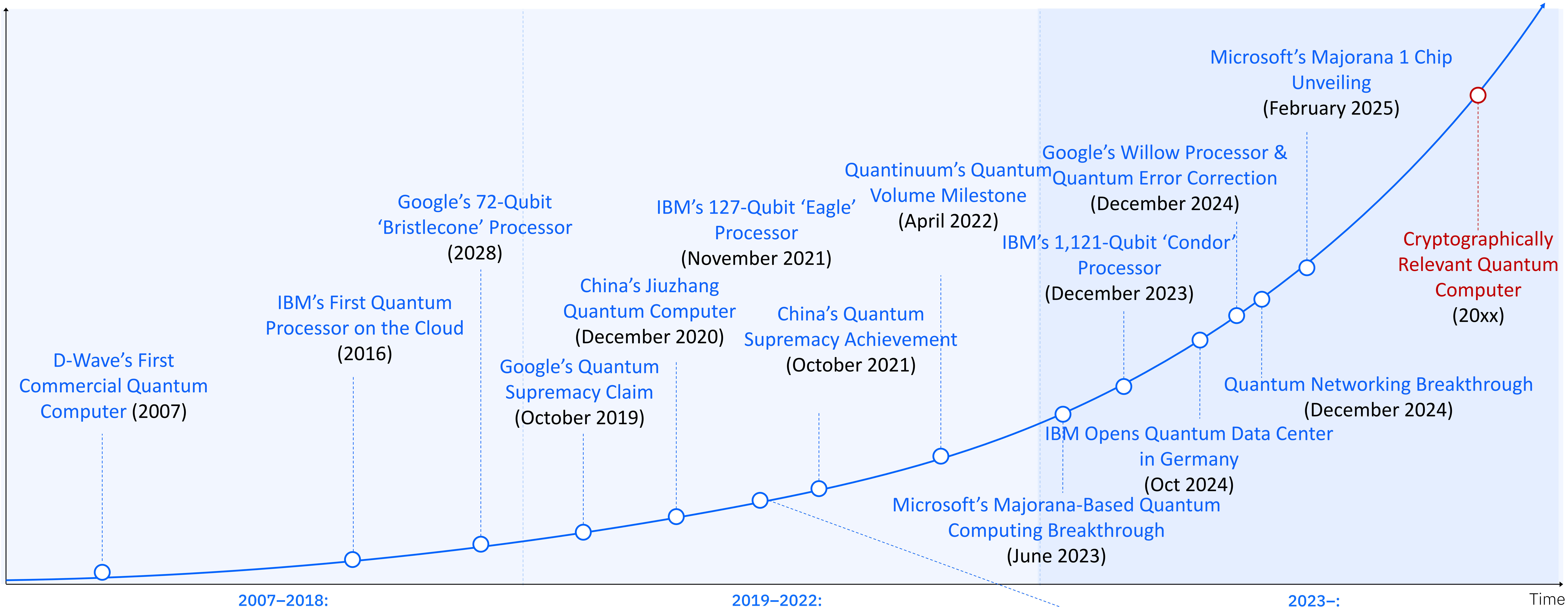
News • January 14, 2025 • 4 min read

2025: The year to become Quantum-Ready

by Mitra Azizirad, President and Chief Operating Officer of Strategic Missions and Technologies @ Microsoft

It’s not if — It’s when

The Quantum Risk –
What’s Happening, and Why It Matters



D-Wave’s First Commercial Quantum Computer (2007)

IBM’s First Quantum Processor on the Cloud (2016)

Google’s 72-Qubit ‘Bristlecone’ Processor (2028)

Google’s Quantum Supremacy Claim (October 2019)

China’s Jiuzhang Quantum Computer (December 2020)

IBM’s 127-Qubit ‘Eagle’ Processor (November 2021)

China’s Quantum Supremacy Achievement (October 2021)

Quantinuum’s Quantum Volume Milestone (April 2022)

Microsoft’s Majorana-Based Quantum Computing Breakthrough (June 2023)

IBM’s 1,121-Qubit ‘Condor’ Processor (December 2023)

IBM Opens Quantum Data Center in Germany (Oct 2024)

Google’s Willow Processor & Quantum Error Correction (December 2024)

Quantum Networking Breakthrough (December 2024)

Microsoft’s Majorana 1 Chip Unveiling (February 2025)

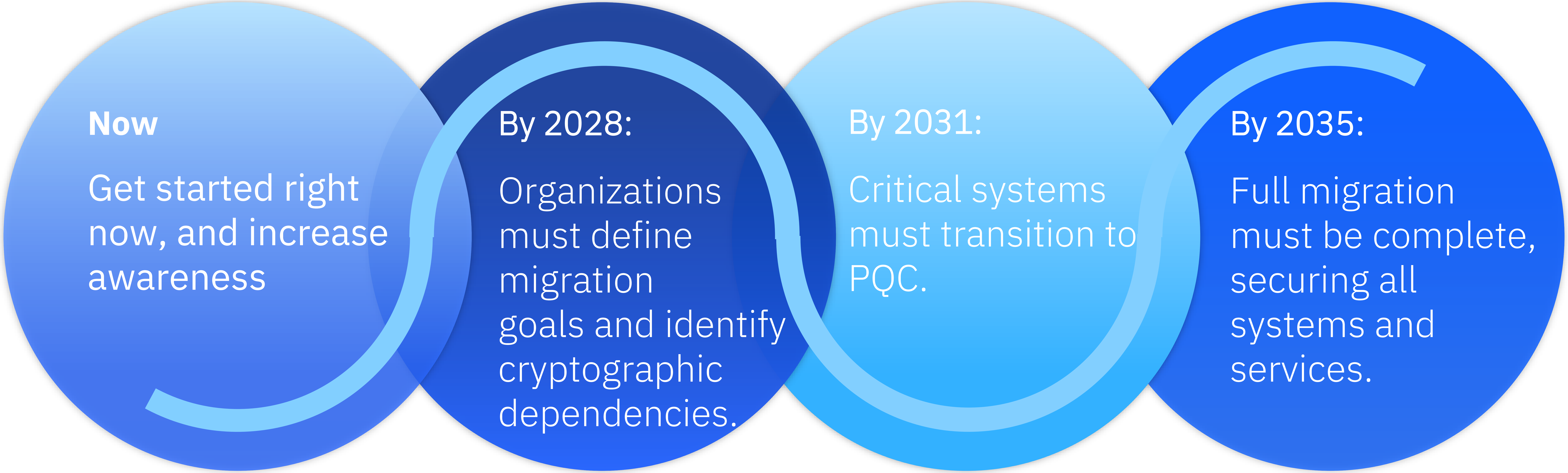
Cryptographically Relevant Quantum Computer (20xx)

2007–2018:
Slow, theoretical progress with small-scale quantum processors and cloud accessibility

2019–2022:
Quantum supremacy milestones, corporate roadmaps, and international infrastructure investments.

2023–:
Accelerated breakthroughs, surpassing 1,000 qubits, quantum networking, and commercialization efforts.

Why Act Now –
The Urgency for Action



Now

Get started right now, and increase awareness

By 2028:

Organizations must define migration goals and identify cryptographic dependencies.

By 2031:

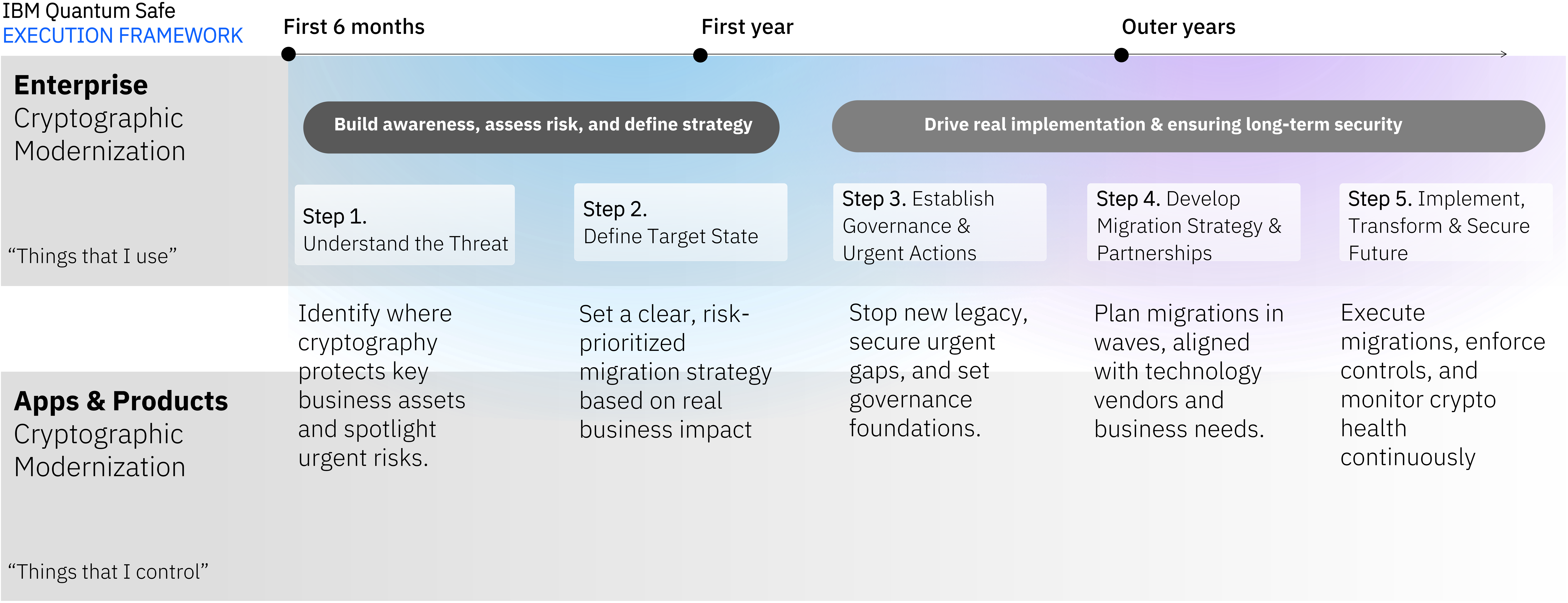
Critical systems must transition to PQC.

By 2035:

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

Peeling the Onion –
A Strategic Approach to Quantum Safe

IBM Quantum Safe
EXECUTION FRAMEWORK



First 6 months

First year

Outer years

Enterprise Cryptographic Modernization

"Things that I use"

Apps & Products Cryptographic Modernization

"Things that I control"

Build awareness, assess risk, and define strategy

Drive real implementation & ensuring long-term security

Step 1. Understand the Threat

Identify where cryptography protects key business assets and spotlight urgent risks.

Step 2. Define Target State

Set a clear, risk-prioritized migration strategy based on real business impact

Step 3. Establish Governance & Urgent Actions

Stop new legacy, secure urgent gaps, and set governance foundations.

Step 4. Develop Migration Strategy & Partnerships

Plan migrations in waves, aligned with technology vendors and business needs.

Step 5. Implement, Transform & Secure Future

Execute migrations, enforce controls, and monitor crypto health continuously

Quantum Safe and the Board

Framing the Business Case

#1 Proactive Migration

#2 Reactive Breach + Regulatory Fines

#3 Loss of Customer Trust

Organizing the Journey

It Takes a Village

Senior Leadership

Compliance and Risk Management Officers

Procurement and Sourcing Teams

Quantum Safe Ambassadors

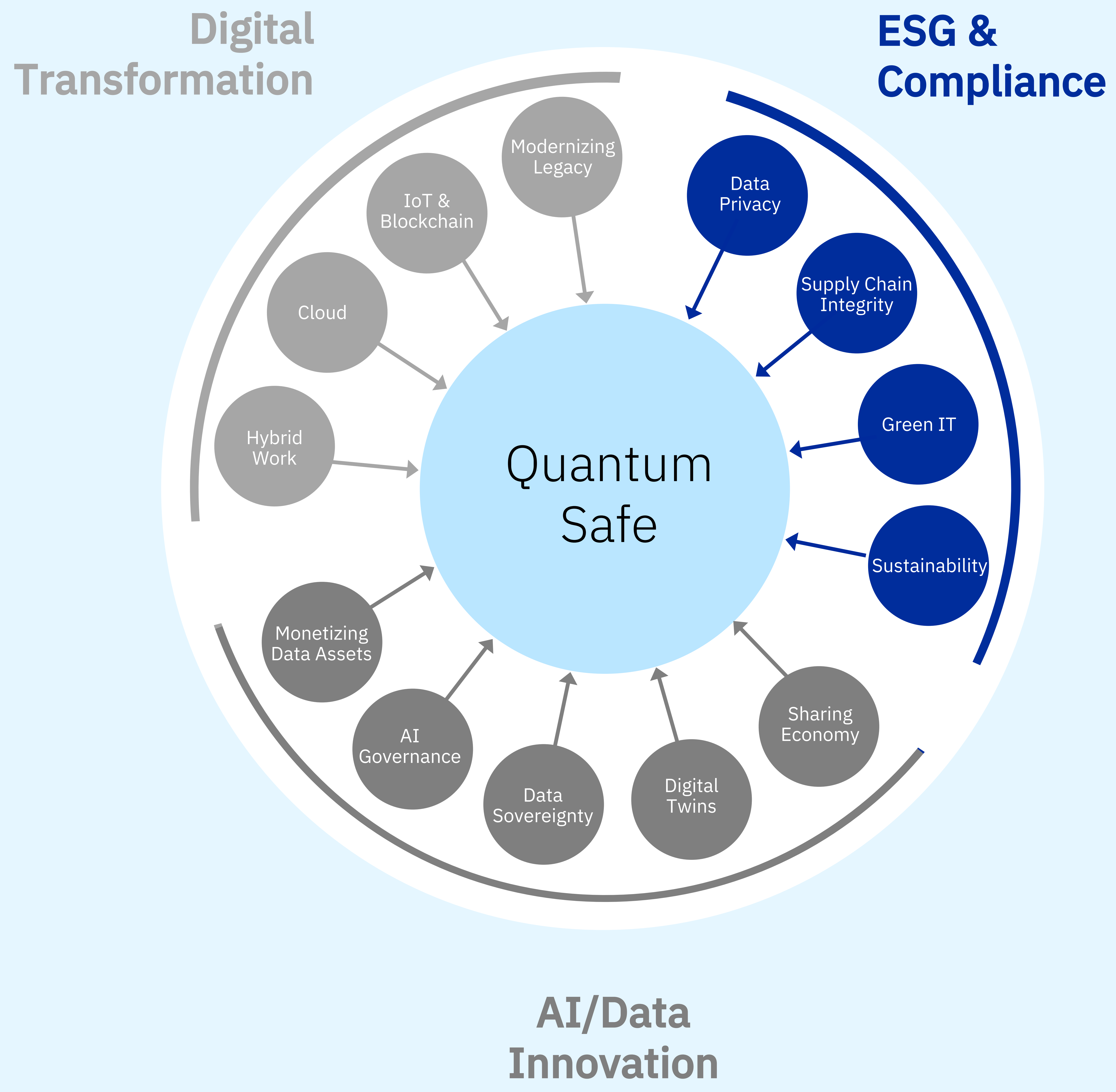
IT Asset / Project Owners

IT and Cybersecurity Teams

3rd party Software and Infrastructure Service Providers

Competing Priorities

How to Tackle It Without Overload



What Happens
If We Wait?

Increased complexity and urgency of migration

Attackers may already be stealing encrypted data

Early adopters gain a strategic edge in security and regulatory compliance

Conclusion & Call to Action

—

Secure the Future, Now

The time to act is now—quantum security transitions take years

Strategize and engage with quantum-safe cryptography initiatives

Invest in partnerships, research, and workforce readiness

The companies that prepare now will lead the post-quantum era

Quantum Safe Landscape

Survey conducted in 2024 and 2025

N = 75 Total Respondents

- 25 Telecommunication brands
- 25 Banking & Financial brands
- 25 Federal Government

Typical Job Title:

- **C-Suite:** CIO, CTO, CISO, CSO…
- **Leaders:** SVP, Director, IT Manager, Architect, Engineer, Developer…

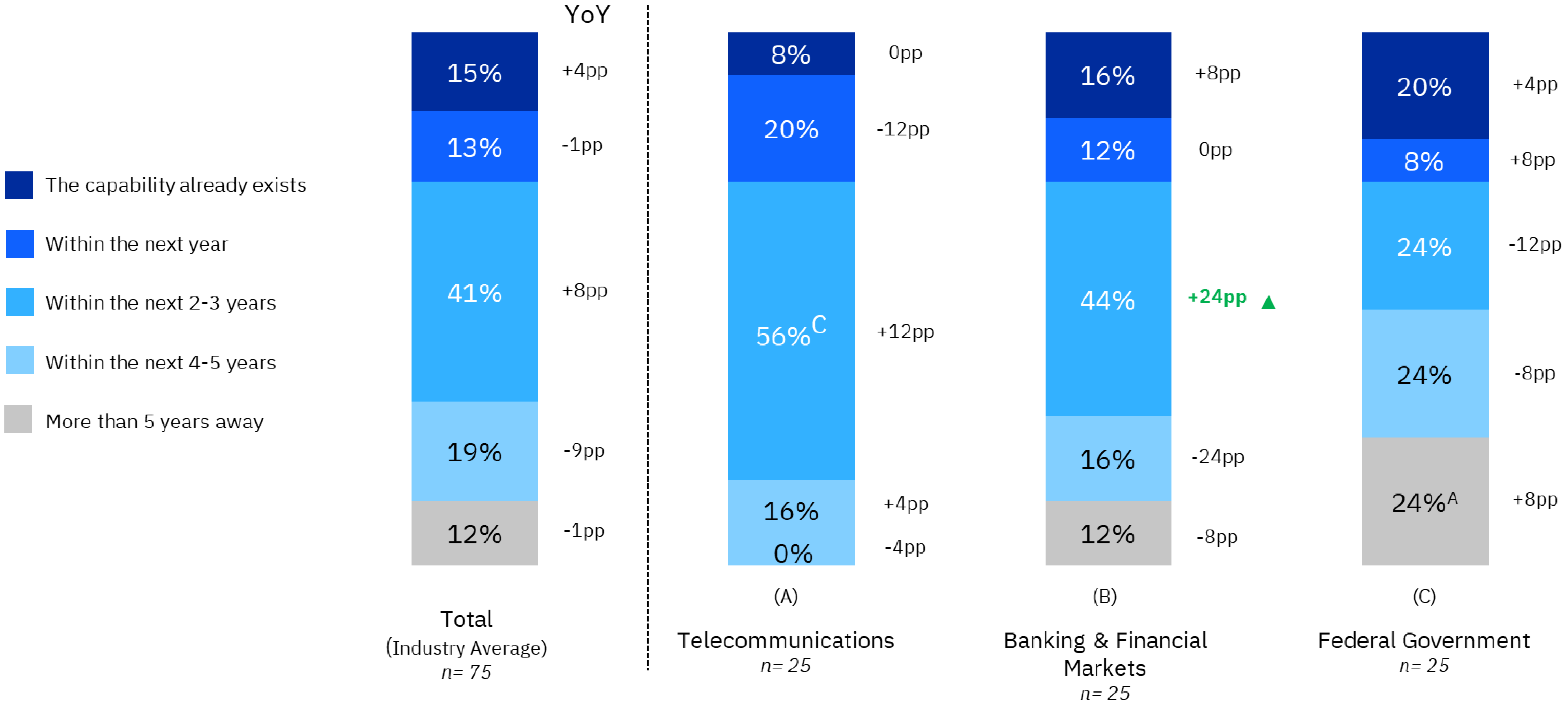
Question: When do you expect that quantum computers will be capable of breaking traditional data security or encryption methods?

56%

Of interviewees believe quantum decryption is 2-3 years away.

28%

Of interviewees expressed extreme concerns towards "Harvest Now Decrypt Later" Risk Attacks



Quantum Safe Landscape

Survey conducted in 2024 and 2025

N = 75 Total Respondents

- •25 Telecommunication brands
- •25 Banking & Financial brands
- •25 Federal Government

Typical Job Title:

- **C-Suite:** CIO, CTO, CISO, CSO…
- **Leaders:** SVP, Director, IT Manager, Architect, Engineer, Developer…

Question: Approximately how many applications is your organization currently using that were developed internally?

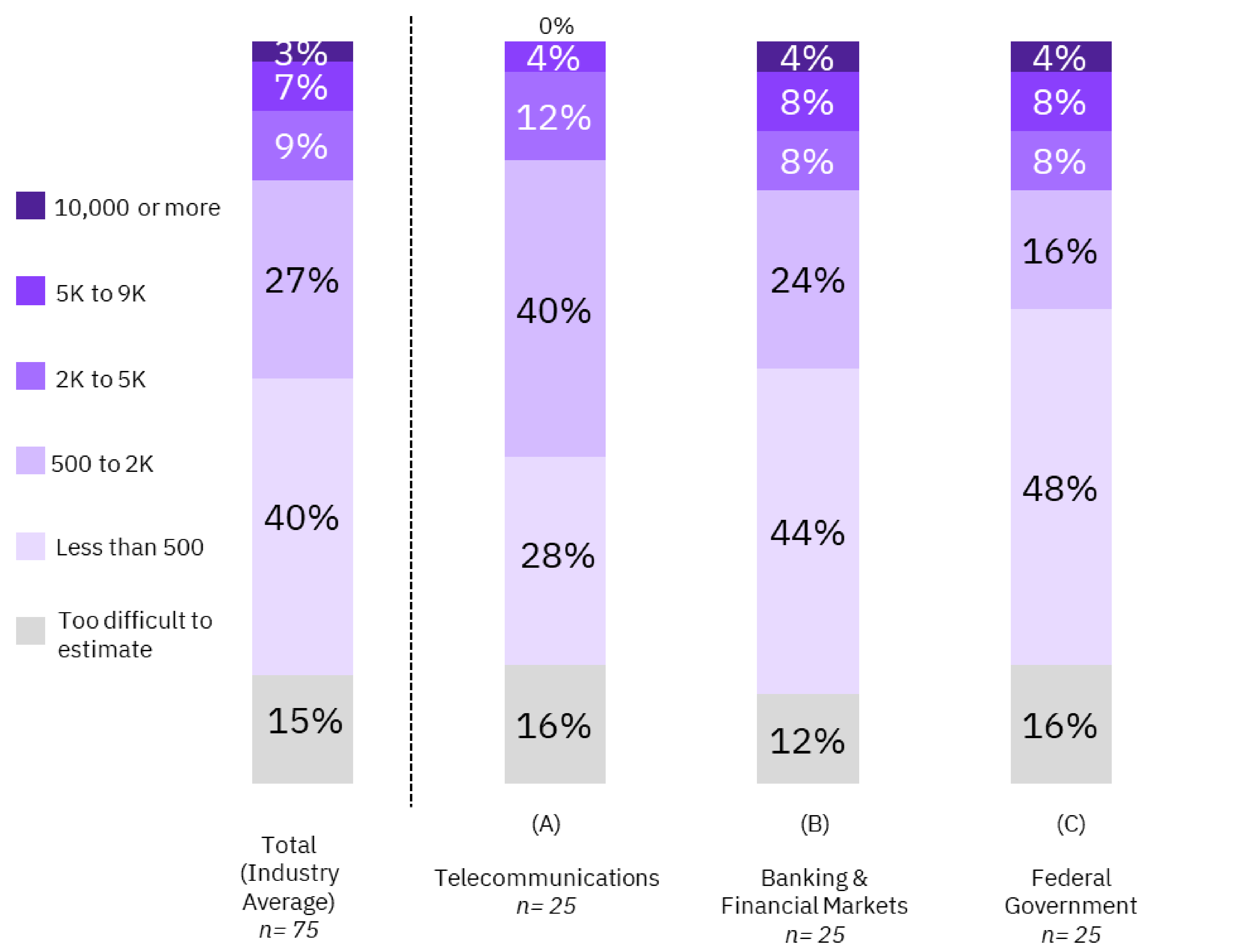
46%

Of organizations run 2000+ self-developed apps — most have not been evaluated for PQC readiness

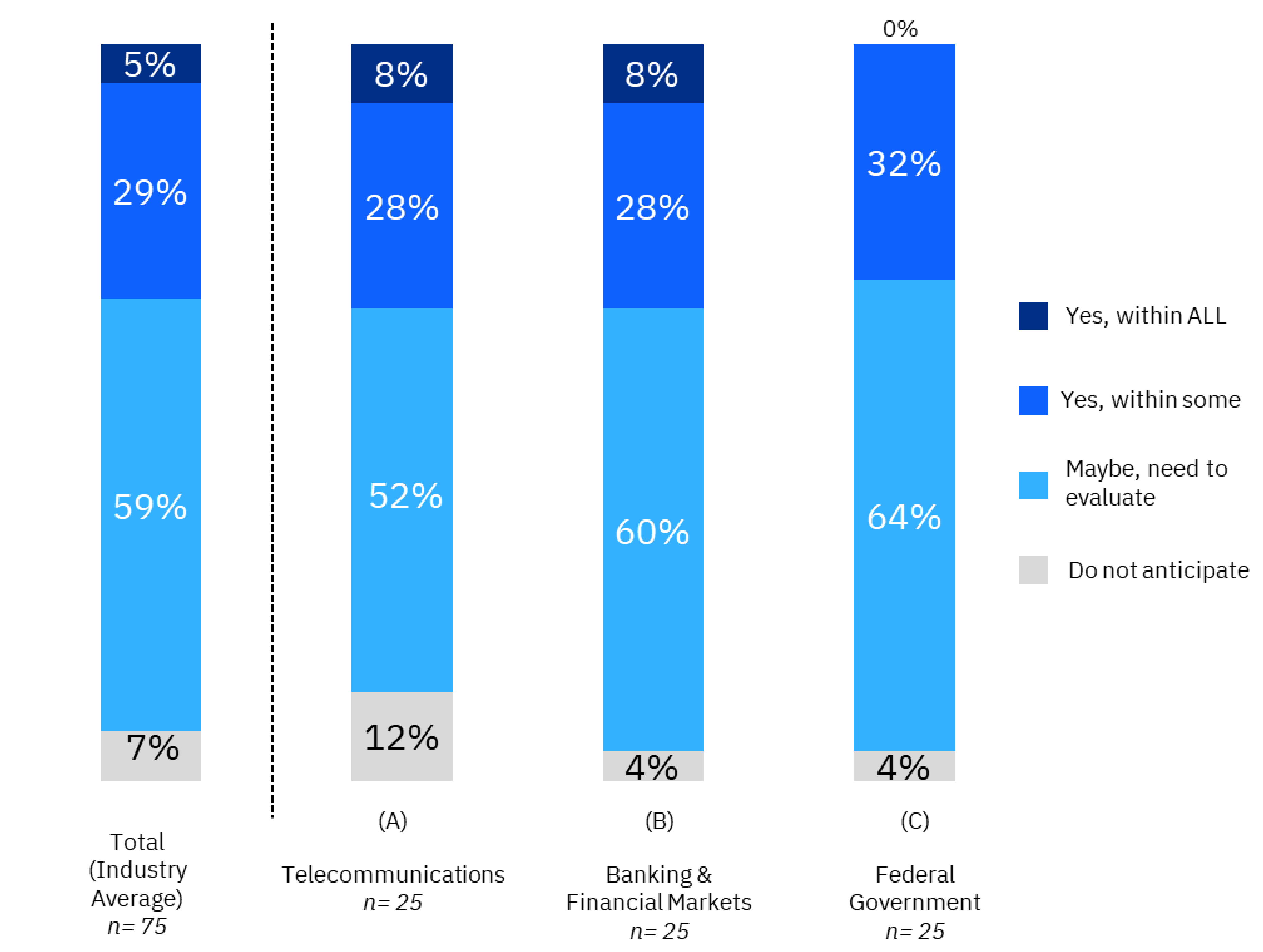
34%

Of interviewees are prioritizing homegrown applications

How many applications is your organization currently using that were developed internally?



Do you anticipate having to deploy PQC solutions within any of your home-grown applications?



Column Letters A,B,C, signify significant difference across industries at the 90% Confidence Interval

Quantum Safe Landscape

30 Minute Survey conducted from December 2024 – February 2025

N = 75 Total Respondents

- 25 Telecommunication brands
- 25 Banking & Financial brands
- 25 Federal Government

Typical Job Title:

- **C-Suite:** CIO, CTO, CISO, CSO…
- **Leaders:** SVP, Director, IT Manager, Architect, Engineer, Developer…

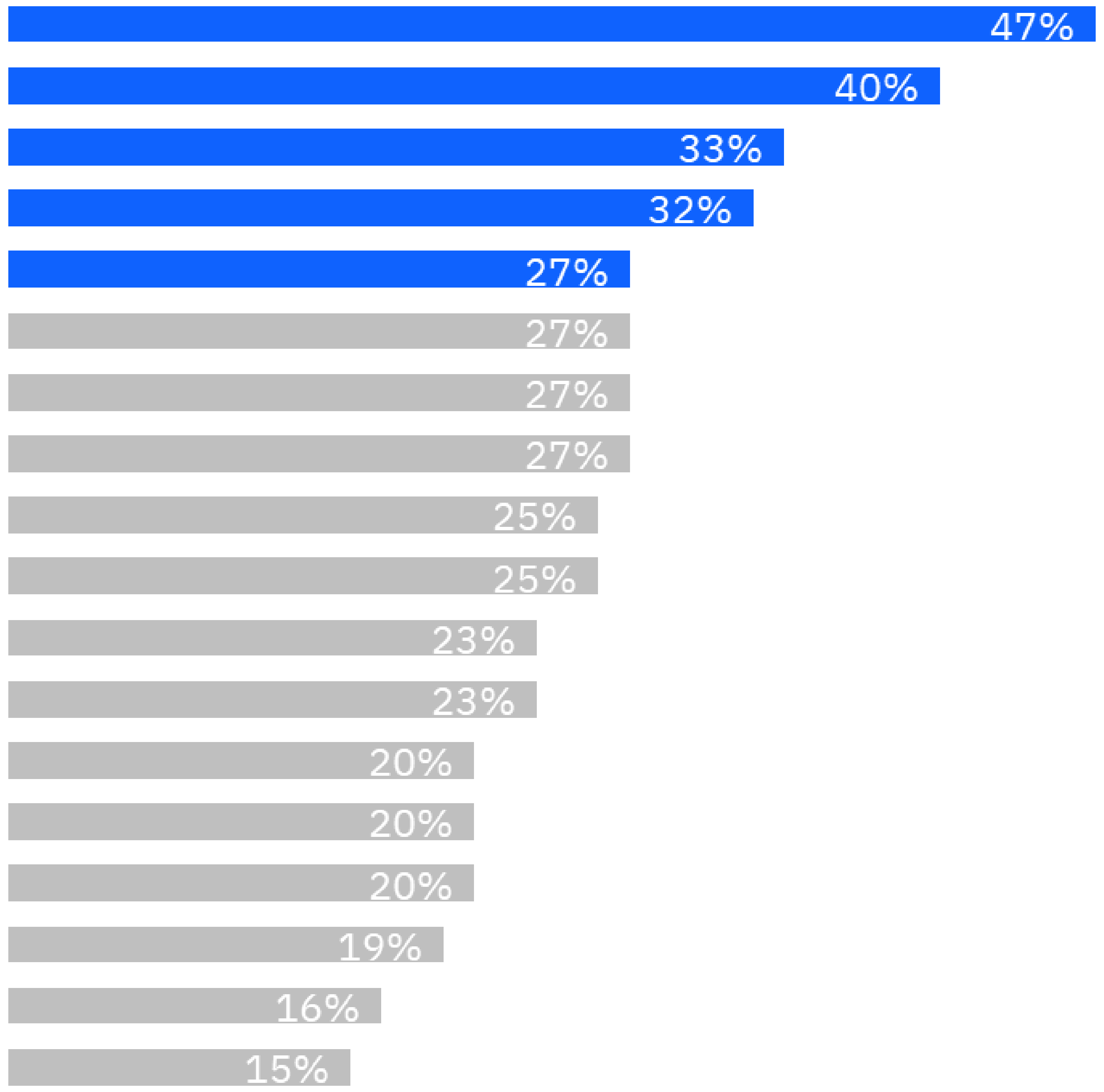
Question: Which of the following are **MOST IMPORTANT** when deciding on PQC solutions?

47%

Of interviewees prioritizes integrations with existing security / system

40%

Of interviewees are prioritizing adherence to standards

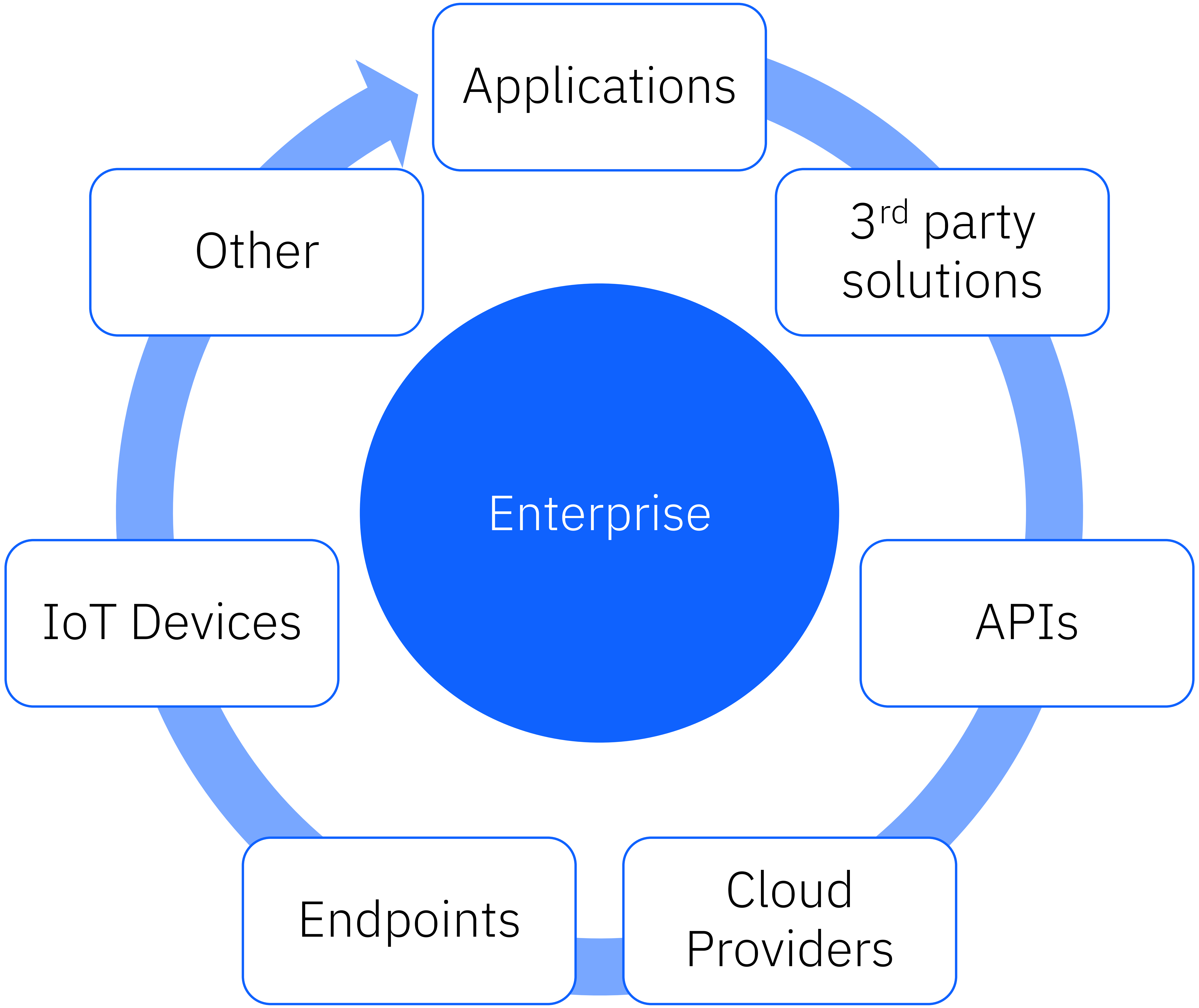


	2025 Ranking	2024 Ranking
PQC Integrates with existing security	#1	#5
Adheres to standards	#2	#3
Assure customers data is quantum safe	#3	#2
Able to address quantum & classical threats	#4	#11
Well established provider of info sec solutions	#5	#10
Applicable use cases	#6	#8
Identify current and future vulnerabilities	#7	#1
Partners to consult best practices	#8	#7
Top Tier experts to advise	#9	#9
Testing prior to full implementation	#10	#13
Supports PQC transformation	#11	#6
Enables crypto-agility	#12	N/A
Training and Educations	#13	#17
Provides future ready applications	#14	#15
Offers ability to bundle	#14	#16
Prioritize where to apply PQC	#15	#14
Leader in PQC	#16	#12
Thought leadership in PQC	#17	#4
	#18	N/A

Enterprises operate with many dependencies

Cryptographic transformation begins with a clear understanding of business objectives, assets, and dependencies, coupled with a strong governance model.

Once we can understand the dependencies, we can assess the risk, prioritize vulnerabilities, and plan remediation actions accordingly.

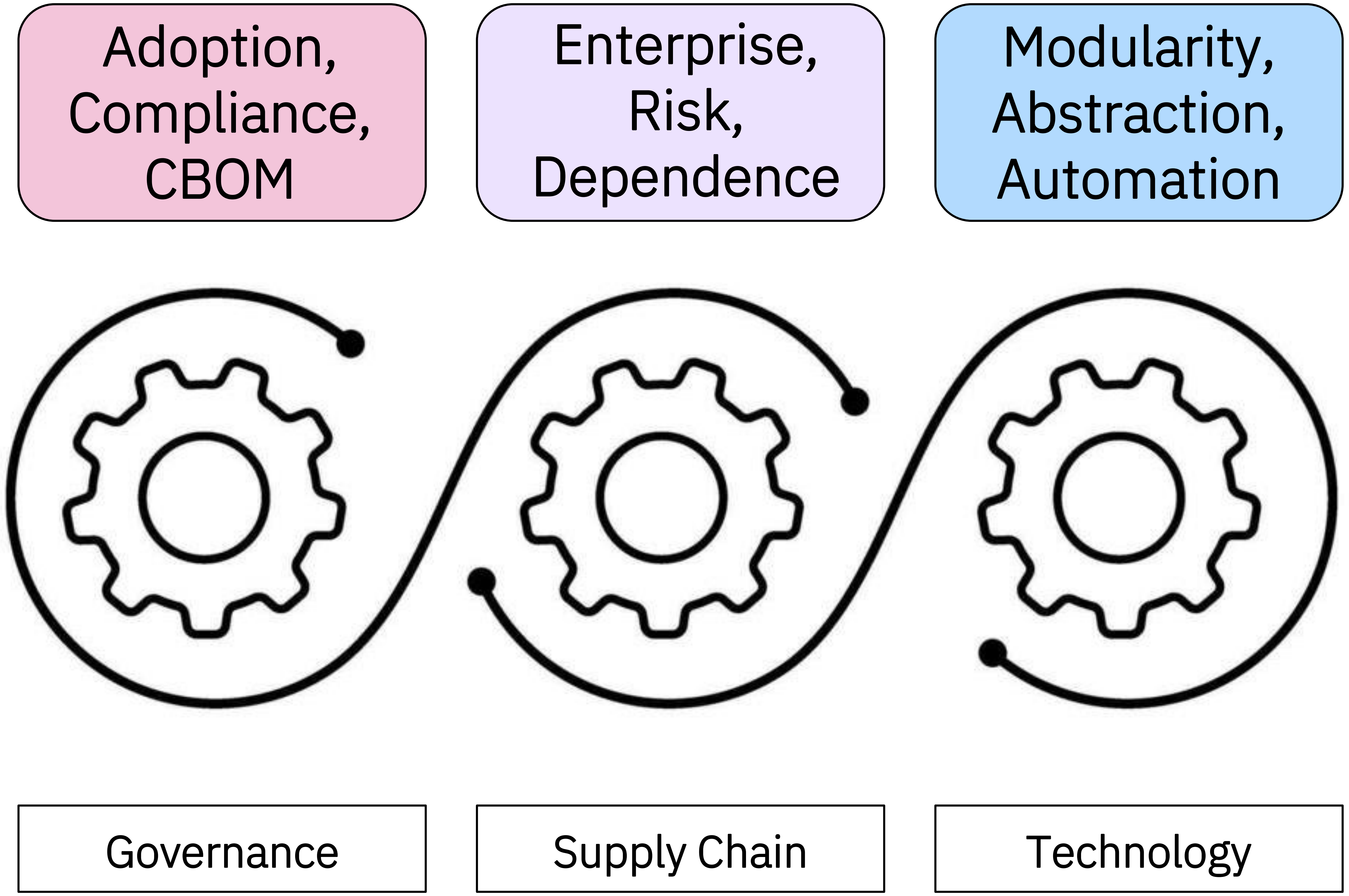


Quantum-safe future requires crypto-agility

What is cryptographic agility?

The **ability** for an organization, platform, system, application, and network **to quickly**:

- **Update** cryptography when it is broken.
- **Change** cryptography when regulations change.
- **Monitor** that cryptography is used properly.
- **Retire** cryptography when it is out of date.



Adoption, Compliance, CBOM

Enterprise, Risk, Dependence

Modularity, Abstraction, Automation

Governance

Supply Chain

Technology

Quantum-safe technologies

Cryptography management for the quantum era

IBM **Quantum** Safe Explorer

Discover cryptography and vulnerabilities in custom applications.

Obtain insights on code-level risks to guide remediation efforts.

Remediate at-risk cryptography by pinpointing precise location in code.

IBM **Guardium** Quantum Safe

Gain visibility into cryptography use across the enterprise network and applications.

Enable faster compliance by applying internal and regulatory policies.

Prioritize vulnerabilities, based on policies, to accelerate remediation actions and track progress.

IBM **Quantum** Safe Remediator

Protect application and network endpoints today without any application changes.

Evaluate the performance of quantum-safe cryptographic algorithms

Mitigate "Harvest Now, Decrypt Later" scenarios

Client scenario:

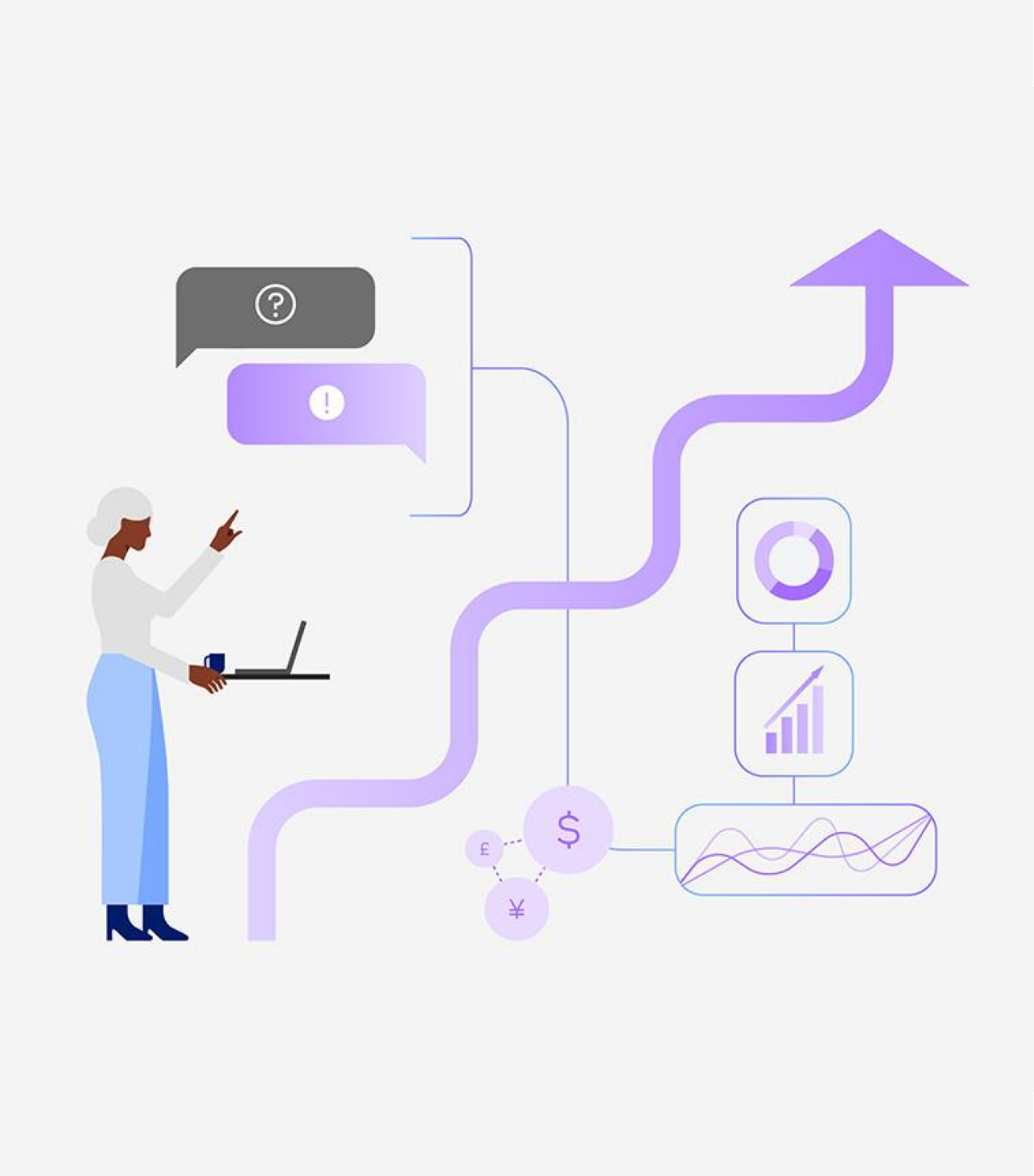
A large global financial institution

Challenge:

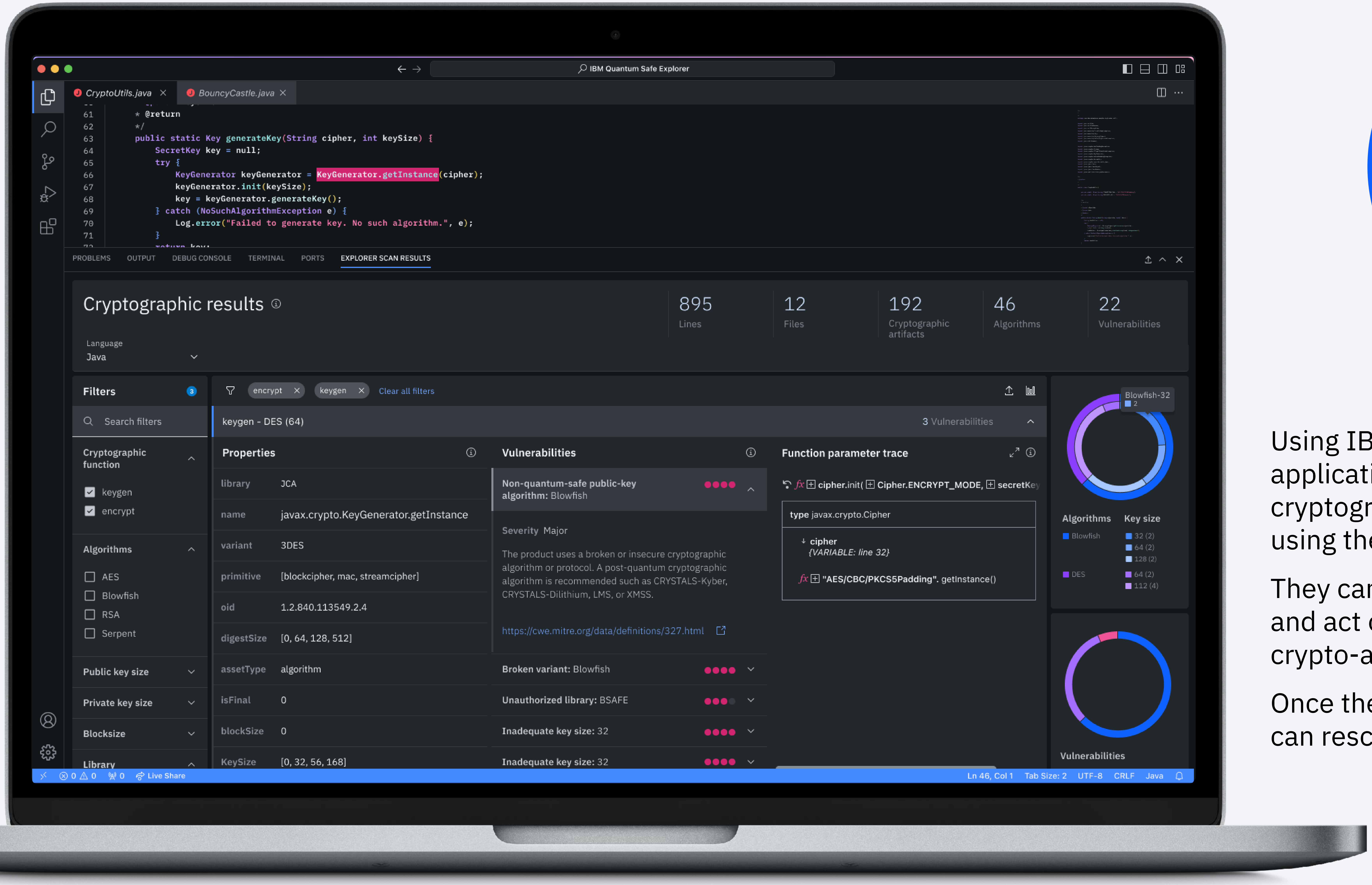
- The client's environment includes 4000+ homegrown applications with cryptography embedded. Without automation, it will be difficult to manage and scale.
- The client stressed for crypto-agility from the beginning and wanted to have solutions in place to achieve their goal.

Approach:

- Scanning all in-house applications and conducting static code analysis through parameter tracing to find code vulnerabilities.
- Developing a plan and prioritization to remediate identified vulnerabilities. Reviewing architecture of business-critical client facing application
- Identifying use of anti-patterns.



IBM Quantum Safe Explorer | Discover cryptography



IBM Quantum Safe Explorer

CryptoUtils.java × | BouncyCastle.java ×

```java
     * @return
     */
    public static Key generateKey(String cipher, int keySize) {
        SecretKey key = null;
        try {
            KeyGenerator keyGenerator = KeyGenerator.getInstance(cipher);
            keyGenerator.init(keySize);
            key = keyGenerator.generateKey();
        } catch (NoSuchAlgorithmException e) {
            Log.error("Failed to generate key. No such algorithm.", e);
        }
        return key;
```

PROBLEMS | OUTPUT | DEBUG CONSOLE | TERMINAL | PORTS | EXPLORER SCAN RESULTS

Cryptographic results ⓘ

895	12	192	46	22
Lines	Files	Cryptographic artifacts	Algorithms	Vulnerabilities

Language: Java

Filters 3

Search filters

Cryptographic function
- ☑ keygen
- ☑ encrypt

Algorithms
- □ AES
- □ Blowfish
- □ RSA
- □ Serpent

Public key size

Private key size

Blocksize

Library

encrypt × | keygen × | Clear all filters

keygen - DES (64) — 3 Vulnerabilities

Properties ⓘ

library	JCA
name	javax.crypto.KeyGenerator.getInstance
variant	3DES
primitive	[blockcipher, mac, streamcipher]
oid	1.2.840.113549.2.4
digestSize	[0, 64, 128, 512]
assetType	algorithm
isFinal	0
blockSize	0
KeySize	[0, 32, 56, 168]

Vulnerabilities ⓘ

Non-quantum-safe public-key algorithm: Blowfish ●●●●

Severity Major

The product uses a broken or insecure cryptographic algorithm or protocol. A post-quantum cryptographic algorithm is recommended such as CRYSTALS-Kyber, CRYSTALS-Dilithium, LMS, or XMSS.

https://cwe.mitre.org/data/definitions/327.html

Broken variant: Blowfish ●●●●

Unauthorized library: BSAFE ●●●○

Inadequate key size: 32 ●●●●

Inadequate key size: 32 ●●●●

Function parameter trace

```
fx ⊞ cipher.init( ⊞ Cipher.ENCRYPT_MODE, ⊞ secretKey
type javax.crypto.Cipher
  ↓ cipher
    {VARIABLE: line 32}
  fx ⊞ "AES/CBC/PKCS5Padding". getInstance()
```

Blowfish-32: 2

Algorithms	Key size
Blowfish	32 (2) 64 (2) 128 (2)
DES	64 (2) 112 (4)

Vulnerabilities

Ln 46, Col 1 | Tab Size: 2 | UTF-8 | CRLF | Java

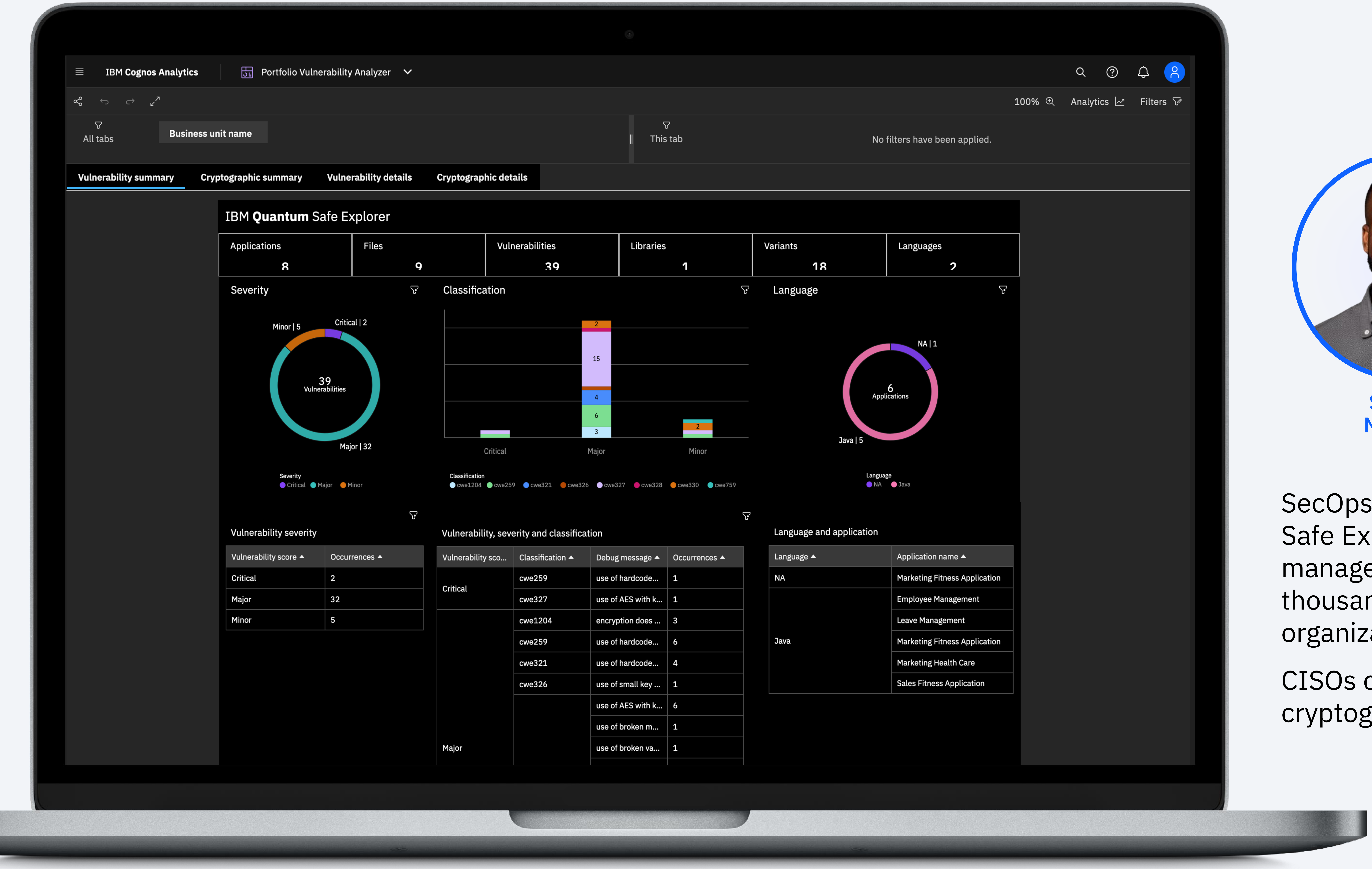
Application Developer

Using IBM Quantum Safe Explorer, application developers can easily discover cryptographic artifacts and vulnerabilities, using these insights to update source code.

They can also identify bad coding practices and act on recommendations to implement crypto-agile best practices.

Once the code has been remediated, they can rescan and validate the results.

IBM Quantum Safe Explorer | Draw insight



IBM **Quantum** Safe Explorer

Applications	Files	Vulnerabilities	Libraries	Variants	Languages
8	9	39	1	18	2

Vulnerability severity

Vulnerability score ▲	Occurrences ▲
Critical	2
Major	32
Minor	5

Vulnerability, severity and classification

Vulnerability sco...	Classification ▲	Debug message ▲	Occurrences ▲
Critical	cwe259	use of hardcode...	1
	cwe327	use of AES with k...	1
Major	cwe1204	encryption does ...	3
	cwe259	use of hardcode...	6
	cwe321	use of hardcode...	4
	cwe326	use of small key ...	1
		use of AES with k...	6
		use of broken m...	1
		use of broken va...	1

Language and application

Language ▲	Application name ▲
NA	Marketing Fitness Application
Java	Employee Management
	Leave Management
	Marketing Fitness Application
	Marketing Health Care
	Sales Fitness Application

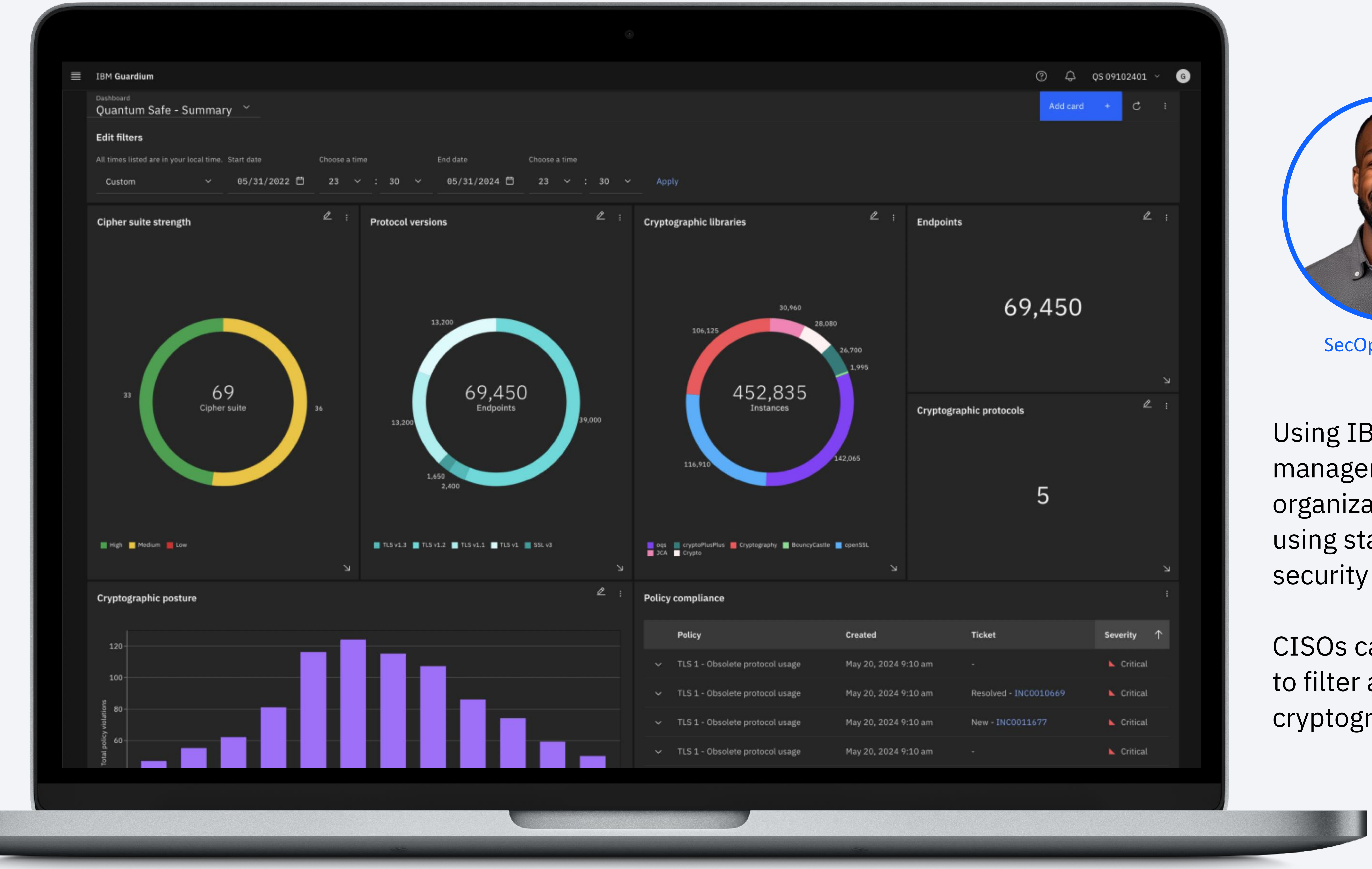
CISO

SecOps Manager

SecOps managers can use IBM Quantum Safe Explorer to aggregate, evaluate, and manage cryptographic vulnerabilities in thousands of applications across their organization to prioritize remediation.

CISOs can filter and track their enterprise's cryptographic posture over time.

IBM Guardium Quantum Safe | Analyze risk posture



IBM Guardium

QS 09102401

Dashboard

Quantum Safe - Summary

Add card +

Edit filters

All times listed are in your local time.

	Start date	Choose a time		End date	Choose a time		
Custom	05/31/2022	23	30	05/31/2024	23	30	Apply

Policy compliance

Policy	Created	Ticket	Severity ↑
TLS 1 - Obsolete protocol usage	May 20, 2024 9:10 am	-	Critical
TLS 1 - Obsolete protocol usage	May 20, 2024 9:10 am	Resolved - INC0010669	Critical
TLS 1 - Obsolete protocol usage	May 20, 2024 9:10 am	New - INC0011677	Critical
TLS 1 - Obsolete protocol usage	May 20, 2024 9:10 am	-	Critical

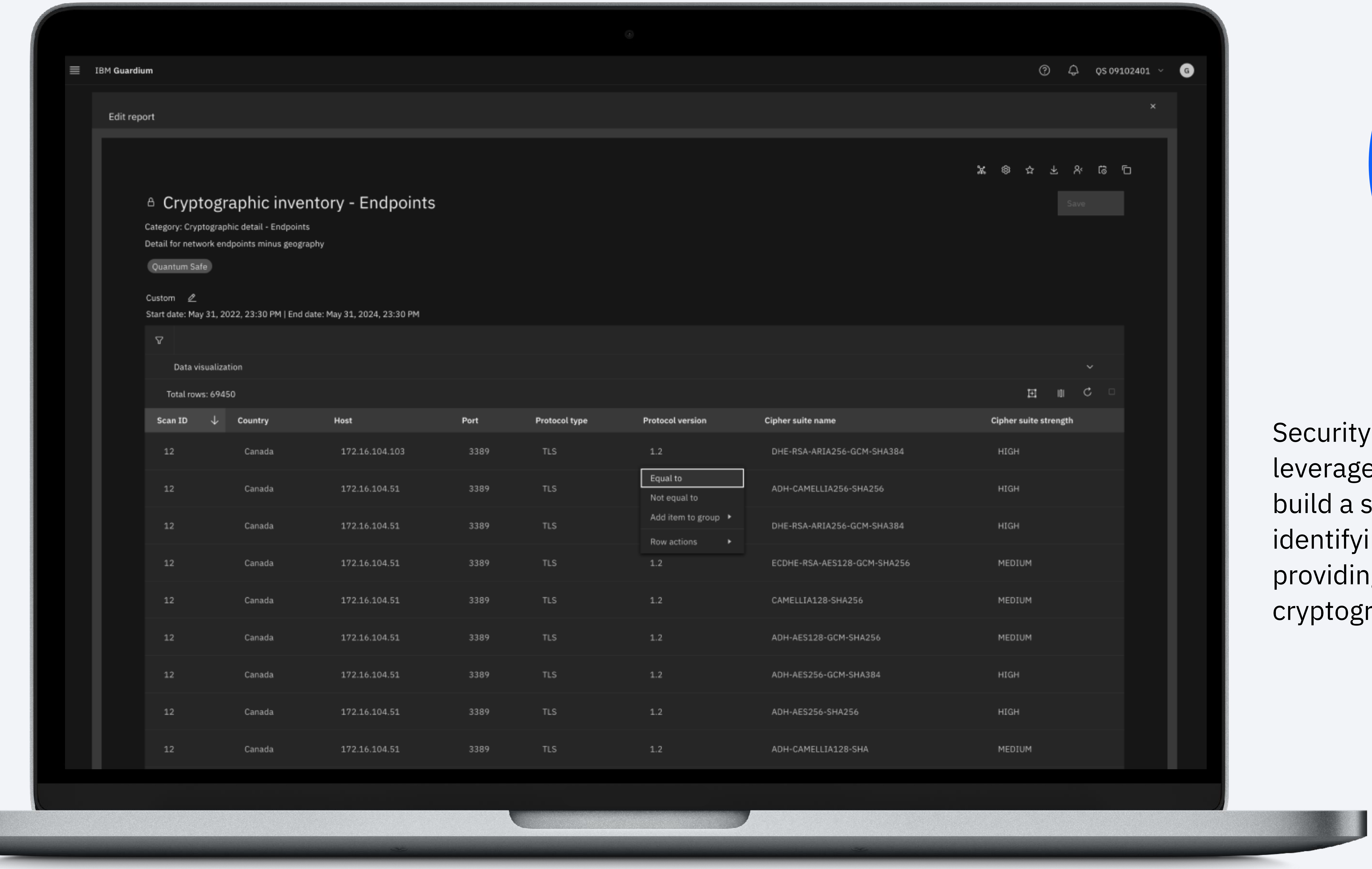
CISO

SecOps Manager

Using IBM Guardium Quantum Safe, SecOps managers can assess and evaluate their organization’s cryptographic risk posture, using standard PQC policies or custom security policies to prioritize remediation.

CISOs can use IBM Guardium Quantum Safe to filter and track their organization’s cryptographic posture over time.

IBM Guardium Quantum Safe | Deepen visibility



Cryptographic inventory - Endpoints

Category: Cryptographic detail - Endpoints

Detail for network endpoints minus geography

Custom

Start date: May 31, 2022, 23:30 PM | End date: May 31, 2024, 23:30 PM

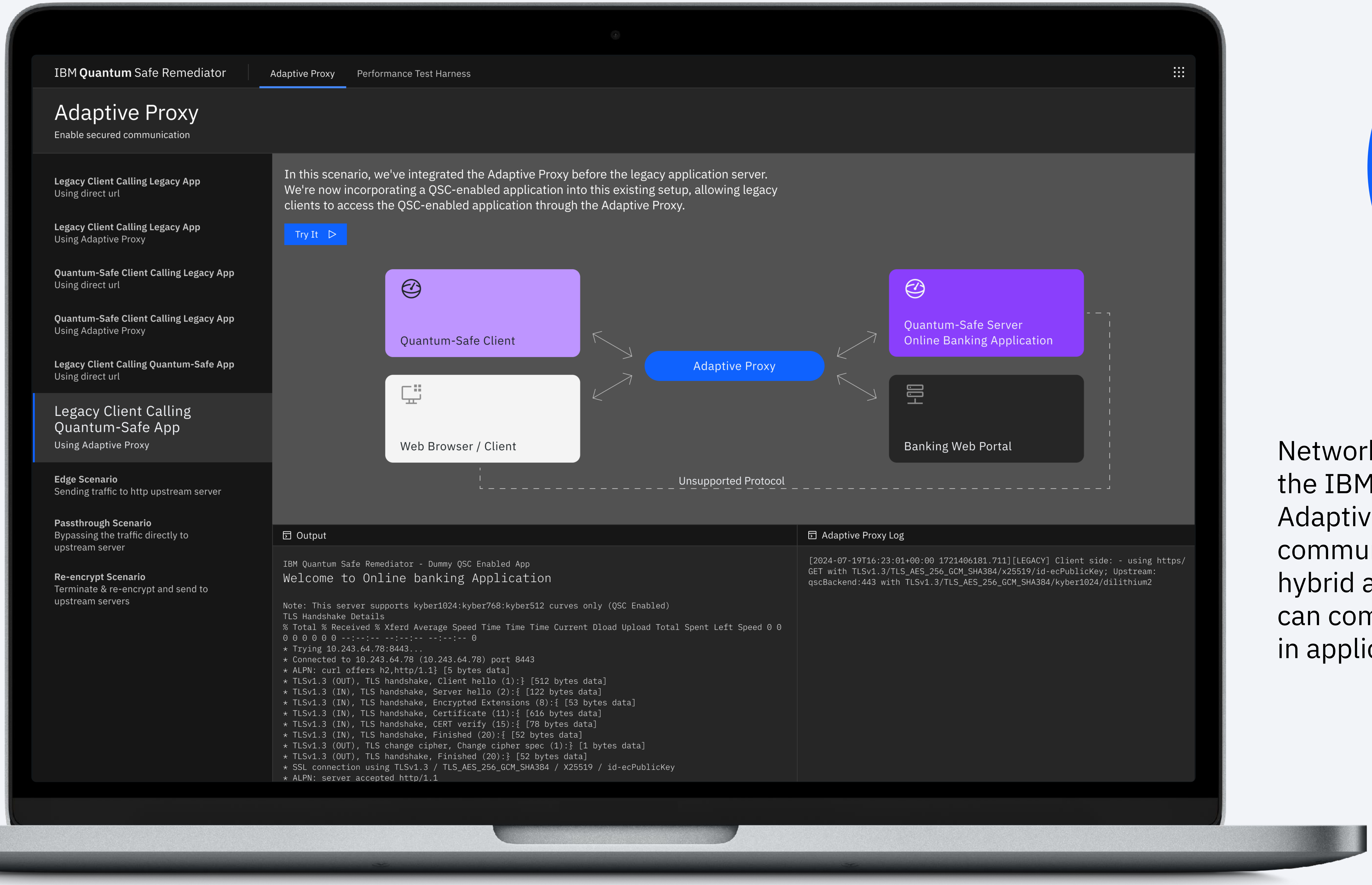
Total rows: 69450

Scan ID	Country	Host	Port	Protocol type	Protocol version	Cipher suite name	Cipher suite strength
12	Canada	172.16.104.103	3389	TLS	1.2	DHE-RSA-ARIA256-GCM-SHA384	HIGH
12	Canada	172.16.104.51	3389	TLS		ADH-CAMELLIA256-SHA256	HIGH
12	Canada	172.16.104.51	3389	TLS		DHE-RSA-ARIA256-GCM-SHA384	HIGH
12	Canada	172.16.104.51	3389	TLS	1.2	ECDHE-RSA-AES128-GCM-SHA256	MEDIUM
12	Canada	172.16.104.51	3389	TLS	1.2	CAMELLIA128-SHA256	MEDIUM
12	Canada	172.16.104.51	3389	TLS	1.2	ADH-AES128-GCM-SHA256	MEDIUM
12	Canada	172.16.104.51	3389	TLS	1.2	ADH-AES256-GCM-SHA384	HIGH
12	Canada	172.16.104.51	3389	TLS	1.2	ADH-AES256-SHA256	HIGH
12	Canada	172.16.104.51	3389	TLS	1.2	ADH-CAMELLIA128-SHA	MEDIUM

Security Infrastructure Architect

Security Infrastructure Architects can leverage IBM Guardium Quantum Safe to build a strong security strategy around identifying and mitigating potential risks by providing visibility into and prioritization of cryptographic vulnerabilities.

IBM Quantum Safe Remediator | Adaptive Proxy



Adaptive Proxy

Enable secured communication

- **Legacy Client Calling Legacy App**
  Using direct url
- **Legacy Client Calling Legacy App**
  Using Adaptive Proxy
- **Quantum-Safe Client Calling Legacy App**
  Using direct url
- **Quantum-Safe Client Calling Legacy App**
  Using Adaptive Proxy
- **Legacy Client Calling Quantum-Safe App**
  Using direct url
- **Legacy Client Calling Quantum-Safe App**
  Using Adaptive Proxy
- **Edge Scenario**
  Sending traffic to http upstream server
- **Passthrough Scenario**
  Bypassing the traffic directly to upstream server
- **Re-encrypt Scenario**
  Terminate & re-encrypt and send to upstream servers

In this scenario, we've integrated the Adaptive Proxy before the legacy application server. We're now incorporating a QSC-enabled application into this existing setup, allowing legacy clients to access the QSC-enabled application through the Adaptive Proxy.

Output

```
IBM Quantum Safe Remediator - Dummy QSC Enabled App
Welcome to Online banking Application

Note: This server supports kyber1024:kyber768:kyber512 curves only (QSC Enabled)
TLS Handshake Details
% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed 0 0
0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0
* Trying 10.243.64.78:8443...
* Connected to 10.243.64.78 (10.243.64.78) port 8443
* ALPN: curl offers h2,http/1.1} [5 bytes data]
* TLSv1.3 (OUT), TLS handshake, Client hello (1):} [512 bytes data]
* TLSv1.3 (IN), TLS handshake, Server hello (2):{ [122 bytes data]
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):{ [53 bytes data]
* TLSv1.3 (IN), TLS handshake, Certificate (11):{ [616 bytes data]
* TLSv1.3 (IN), TLS handshake, CERT verify (15):{ [78 bytes data]
* TLSv1.3 (IN), TLS handshake, Finished (20):{ [52 bytes data]
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):} [1 bytes data]
* TLSv1.3 (OUT), TLS handshake, Finished (20):} [52 bytes data]
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384 / X25519 / id-ecPublicKey
* ALPN: server accepted http/1.1
```

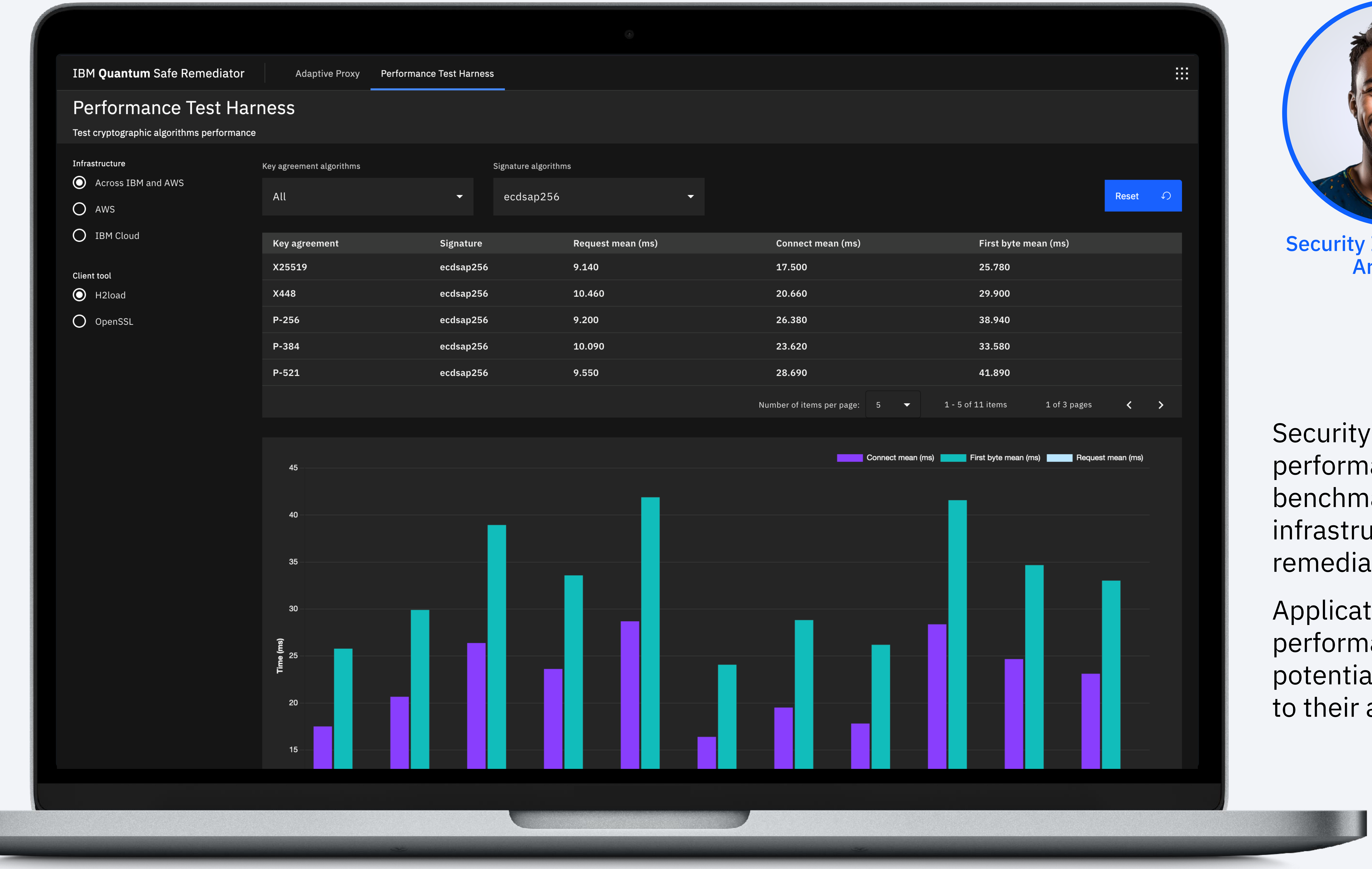
Adaptive Proxy Log

```
[2024-07-19T16:23:01+00:00 1721406181.711][LEGACY] Client side: - using https/
GET with TLSv1.3/TLS_AES_256_GCM_SHA384/x25519/id-ecPublicKey; Upstream:
qscBackend:443 with TLSv1.3/TLS_AES_256_GCM_SHA384/kyber1024/dilithium2
```

Network Security Administrator

Network security administrators can use the IBM Quantum Safe Remediator Adaptive Proxy to configure communication, ensuring clients using hybrid and PQC encryption algorithms can communicate without changing code in applications.

IBM Quantum Safe Remediator | Performance harness



Performance Test Harness

Test cryptographic algorithms performance

Infrastructure

● Across IBM and AWS

○ AWS

○ IBM Cloud

Client tool

● H2load

○ OpenSSL

Key agreement algorithms: All

Signature algorithms: ecdsap256

Key agreement	Signature	Request mean (ms)	Connect mean (ms)	First byte mean (ms)
X25519	ecdsap256	9.140	17.500	25.780
X448	ecdsap256	10.460	20.660	29.900
P-256	ecdsap256	9.200	26.380	38.940
P-384	ecdsap256	10.090	23.620	33.580
P-521	ecdsap256	9.550	28.690	41.890

Number of items per page: 5   1 - 5 of 11 items   1 of 3 pages

Security Infrastructure Architect

Application Developer

Security infrastructure architects can use the performance test harness to view benchmark data and understand impact on infrastructure performance so they can make remediation recommendations to the CISO.

Application developers can use the performance test harness to understand the potential impact of recommended upgrades to their applications prior to making changes.

What should organizations do next?

Consider your quantum-safe readiness →

https://ibm.biz/BdKmzS

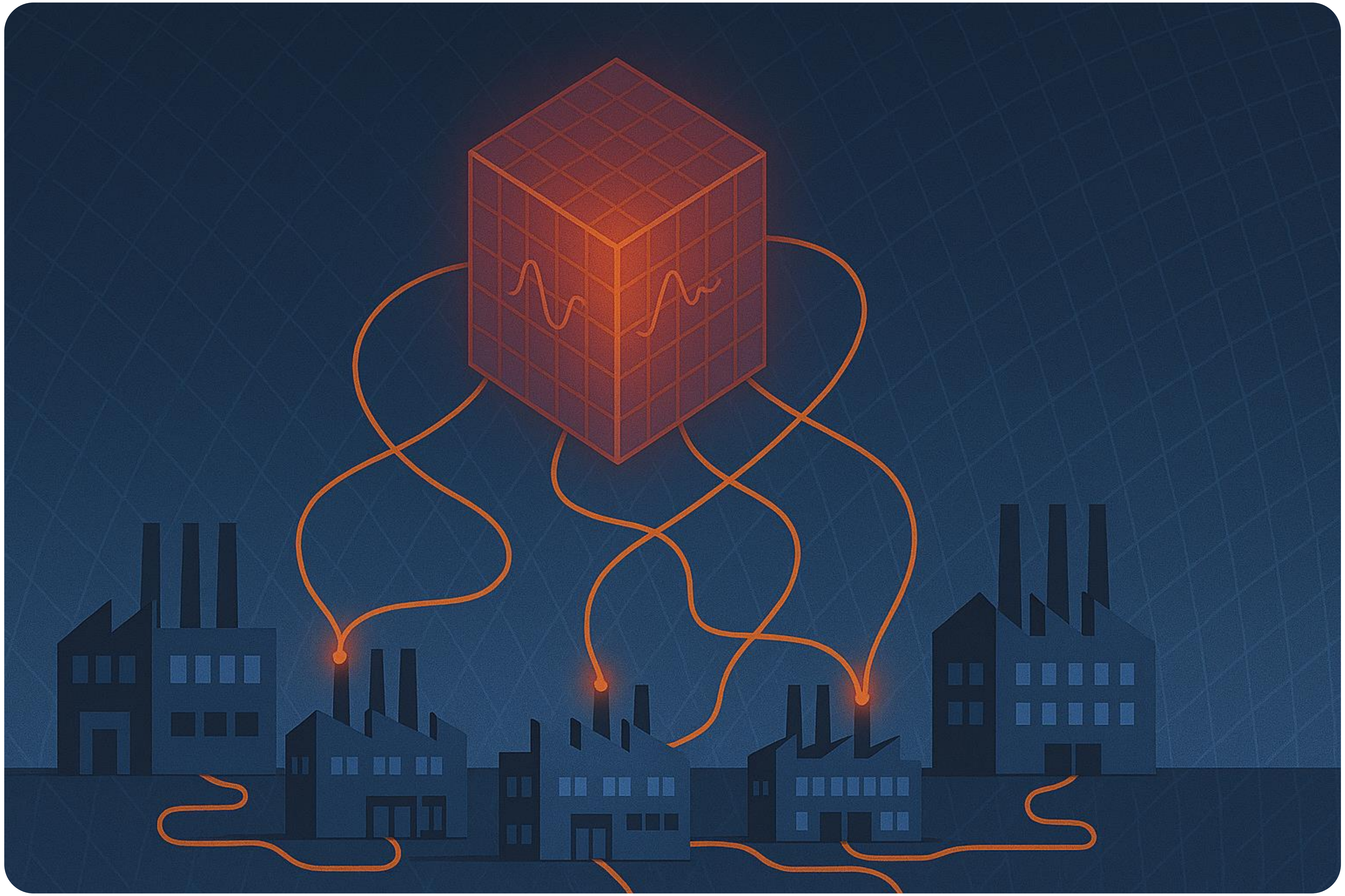
Discover and observe cryptography across your enterprise IT landscape.

Establish cryptographic governance within your enterprise and across the supply chain.

Begin migrating to post-quantum cryptography using code and network remediation practices.

Get involved with quantum-safe consortia to stay up to date on best practices for implementation.

Why Collaboration Matters in the Quantum Era



What Industry Collaboration Looks Like

Sharing threat models

Coordinating migration patterns

Engaging in open standards

Collectively shaping procurement expectations

NACHA The Electronic Payments Association

EPA ASIA

EUROPOL

MITRE

ETSI

Post-Quantum Cryptography Alliance

GSMA

FS-ISAC

Future-Proofing

Data Security

1 Stop creating net-new legacy now

2 Prioritize long-lived data & assets

3 Build agile, risk-based migration programs

4 Think in waves

Your Organization's
Next Steps

Enterprise and Platform Cryptographic Posture

Application and Product Cryptographic Posture

First 3-6 months

Step 1.
Understand the Threat

Conduct high-level, risk-based impact study

Identify long-lived, high-value systems and data sets

Run threat and business risk-based analysis

Engage with cross-industry collaboration groups to align on best practices

First year

Step 2.
Define Target State

Establish a three-tier cryptography inventory

Define the Quantum Safe target state and fields of action

Develop detailed migration roadmap and justification case

Outer years

Step 3.
Execute Migration

Urgently implement governance, procurement controls, and immediate technical mitigations

Design migration patterns, collaborate with vendors, and roll out phased migration

Enforce control points, and establish continuous cryptographic monitoring

How can IBM help –
What value we bring

Contact us

Strategic Clarity on Quantum Risk

We help clients demystify quantum risk by translating complex cryptographic exposure into clear business impact. Our **award-winning methodology**, combined with **structured migration orchestration platform** and **threat impact analysis**, enables leadership to make informed, risk-based decisions. Unlike others, **we anchor quantum security in real-world business contexts**, not just technology layers.

Accelerated Readiness Through AI-Powered Execution

We drastically reduce time-to-insight by **combining expert consulting with AI and automation**.
Our use of digital workers and **research-led automation tools** allows for rapid discovery of cryptographic assets, scalable risk modeling, and continuous compliance tracking—making us **faster and more scalable** than traditional consulting models.

Seamless Migration with Proven Patterns and Tools

We de-risk and simplify the transition to quantum-safe through **field-tested patterns** and modular **migration frameworks**.
From crypto-agility patterns and **network & cryptography-as-a-servic**e to the **industry's first migration orchestration platform**, our **pre-built solutions** ensure clients can move from planning to execution smoothly, even across complex estates.

Deep Industry Influence and Future-Proof Alignment

We align client roadmaps with global standards and future cryptographic landscapes.
As **contributors to NIST PQC**, founders of i**ndustry consortiums**, and partners in **national-level quantum security initiatives**, we ensure our clients are always aligned with the latest standards, regulatory expectations, and emerging best practices.

IBM