CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023

CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

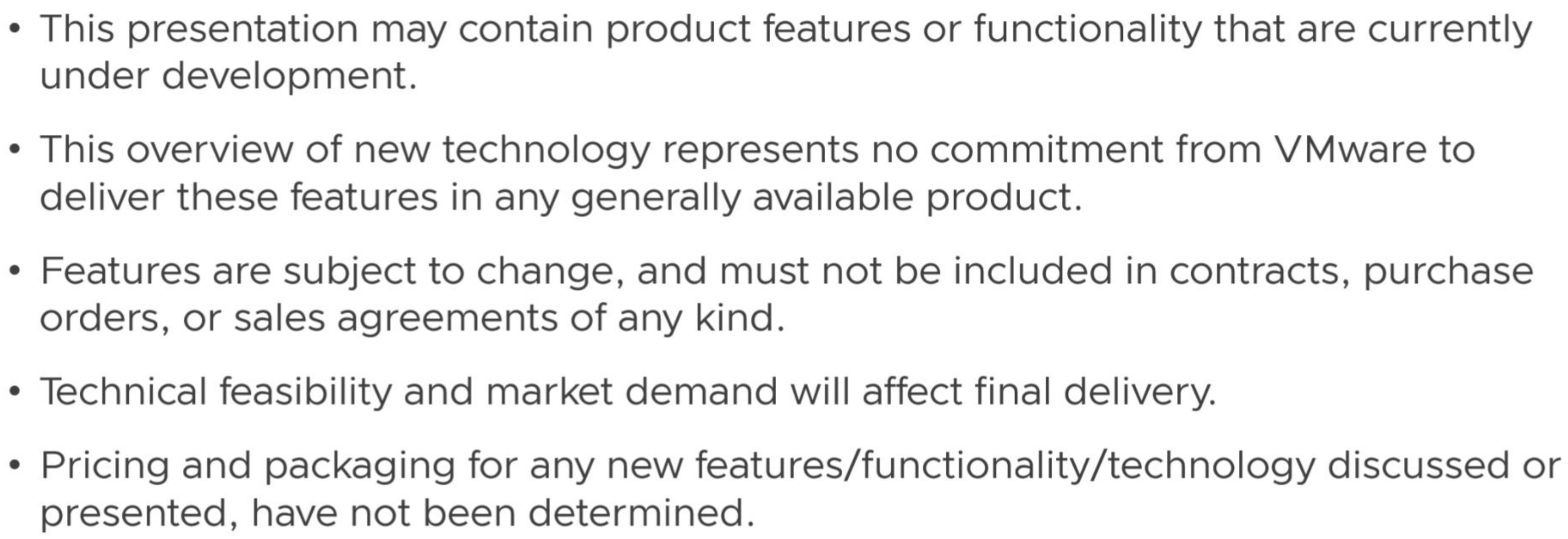
Cryptographic Agility: Preparing Modern Apps for Quantum Safety and Beyond

Natalie Fisher

Agenda

- What is Cryptographic Agility?
- Why do you care?
- How to prepare
- VMware’s Plans

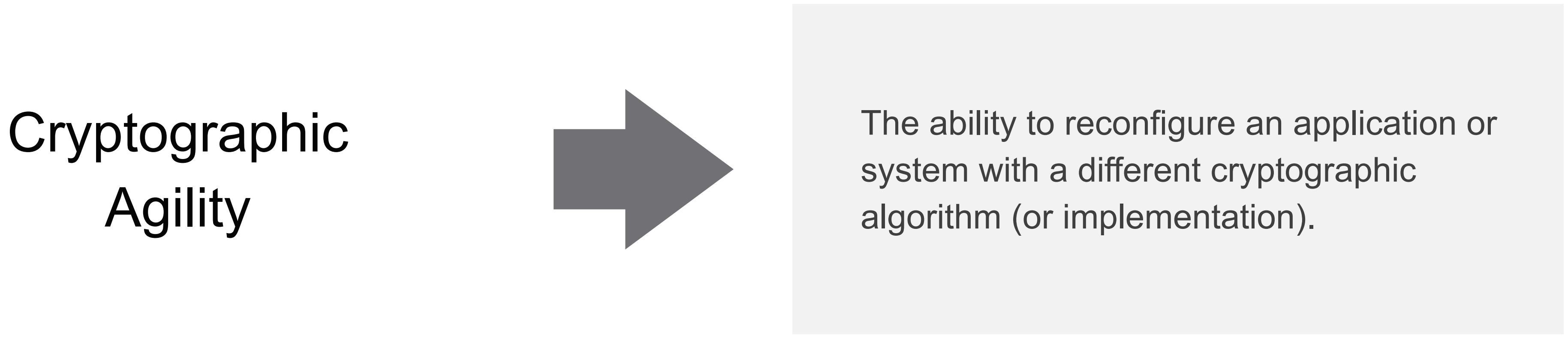
Required Disclaimer



- This presentation may contain product features or functionality that are currently under development.
- This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.
- Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.
- Technical feasibility and market demand will affect final delivery.
- Pricing and packaging for any new features/functionality/technology discussed or presented, have not been determined.

What is Cryptographic Agility?

Cryptographic Agility



Cryptographic Agility

The ability to reconfigure an application or system with a different cryptographic algorithm (or implementation).

Cryptographic Agility Advantages

Transition to New Algorithms

Change Library

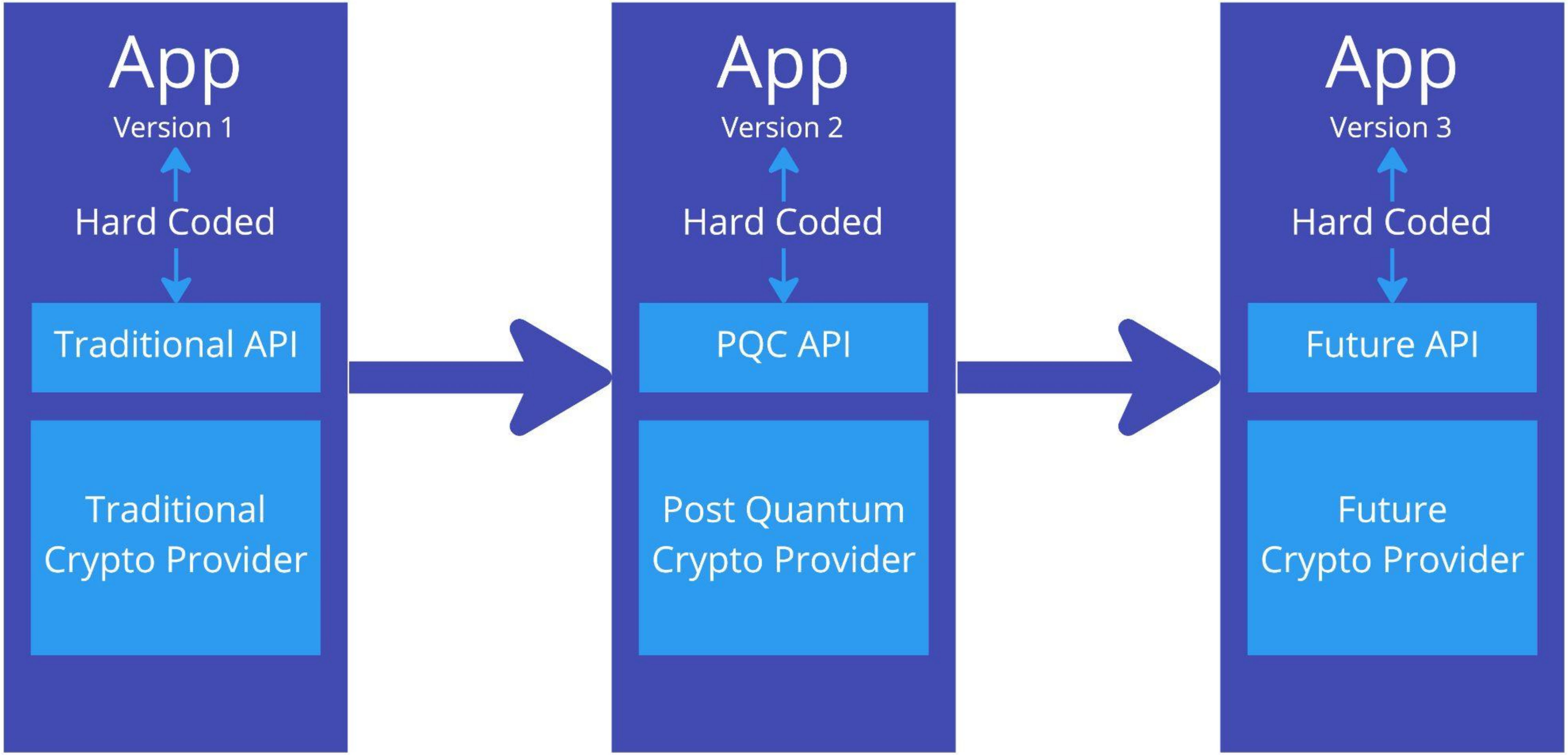
Modifying Config

Retiring Algorithms

Compliance Standards

Streamline Remediation

Current landscape



App

Version 1

Hard Coded

Traditional API

Traditional Crypto Provider

App

Version 2

Hard Coded

PQC API

Post Quantum Crypto Provider

App

Version 3

Hard Coded

Future API

Future Crypto Provider

THIS IS FINE

Current Landscape Problems

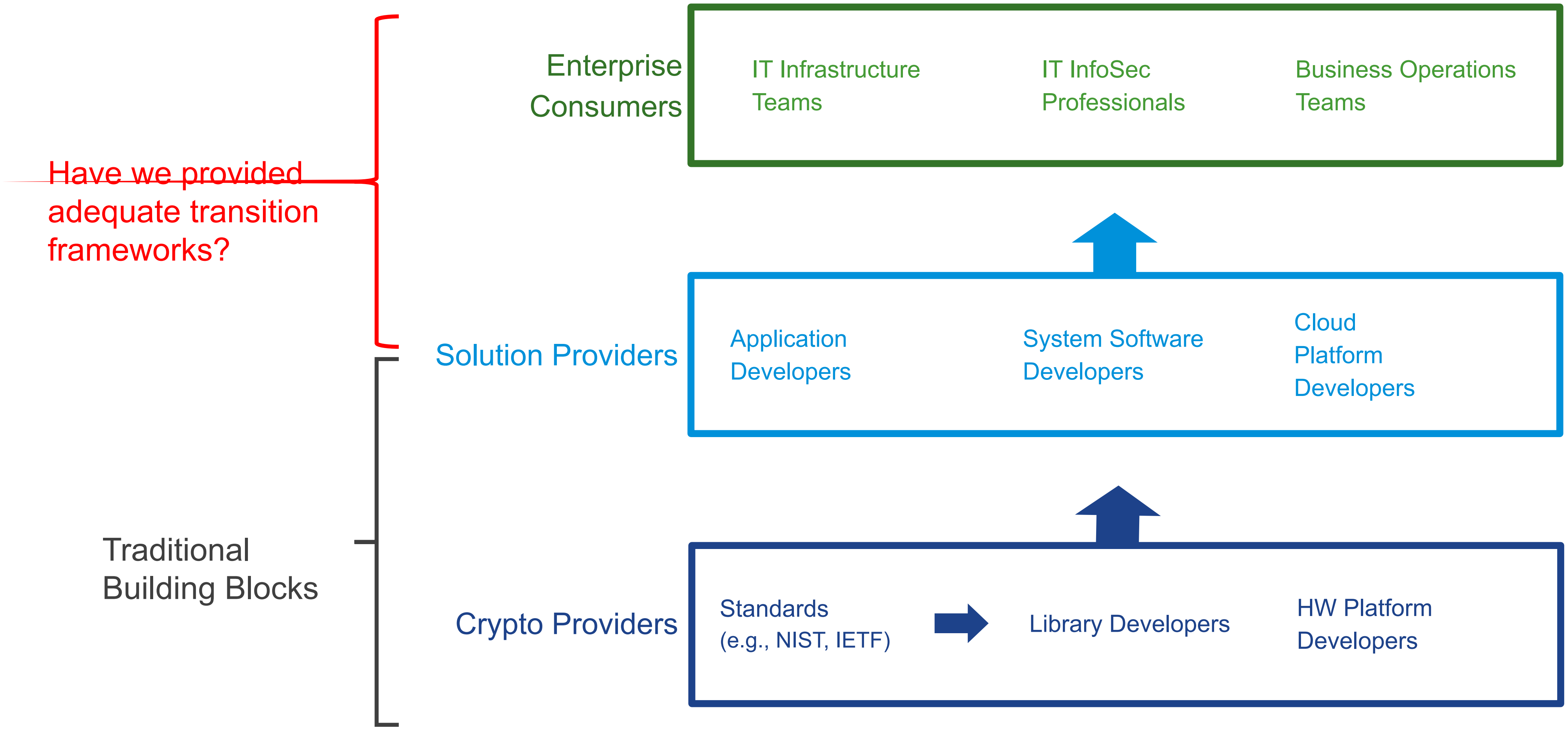
Lack of visibility

No unification

Rearchitecting required

Challenges: The Stakeholders

Are we hearing them?



Have we provided adequate transition frameworks?

Traditional Building Blocks

Enterprise Consumers

- IT Infrastructure Teams
- IT InfoSec Professionals
- Business Operations Teams

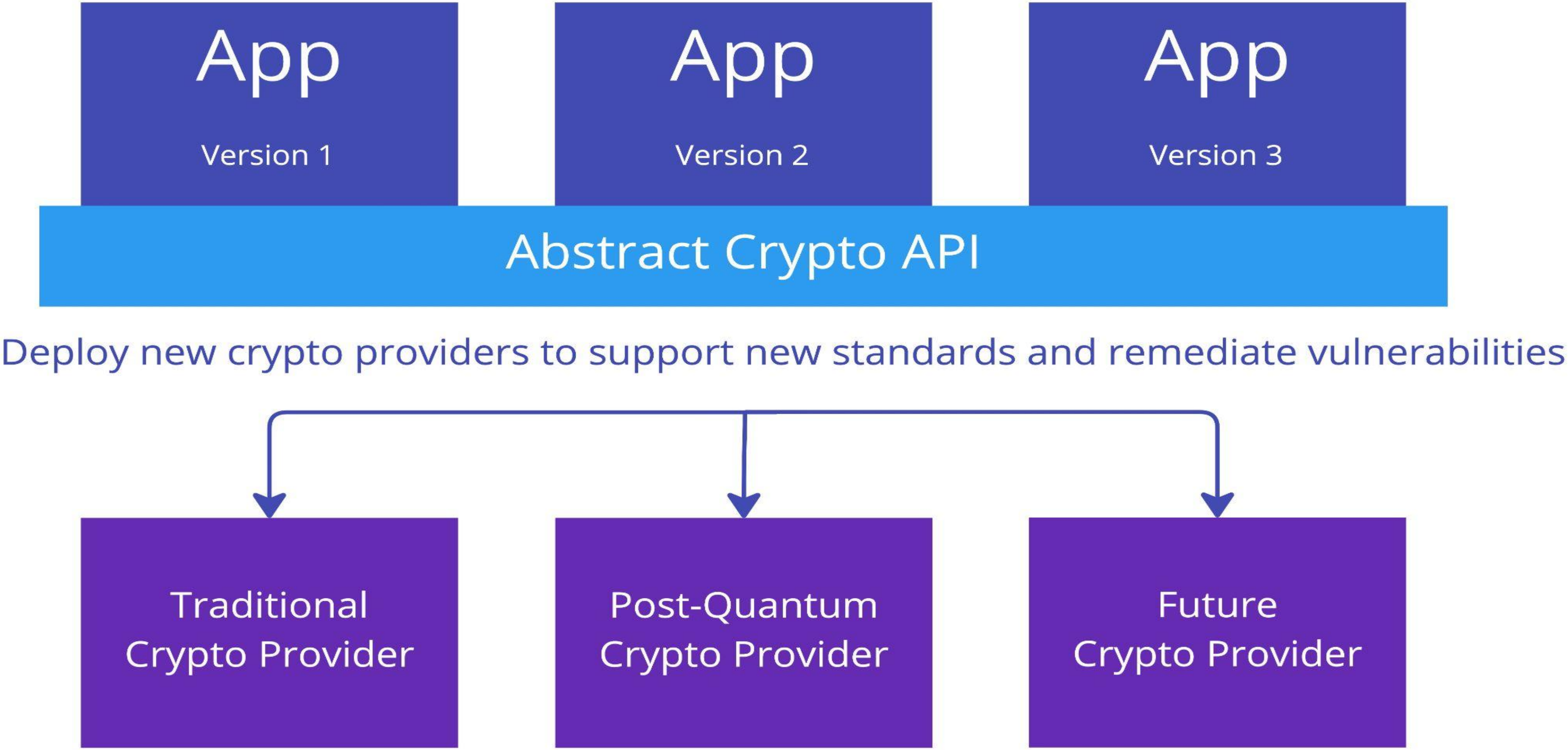
Solution Providers

- Application Developers
- System Software Developers
- Cloud Platform Developers

Crypto Providers

- Standards (e.g., NIST, IETF) → Library Developers
- HW Platform Developers

Future Landscape



App

Version 1

App

Version 2

App

Version 3

Abstract Crypto API

Deploy new crypto providers to support new standards and remediate vulnerabilities

Traditional Crypto Provider

Post-Quantum Crypto Provider

Future Crypto Provider

Future landscape benefits

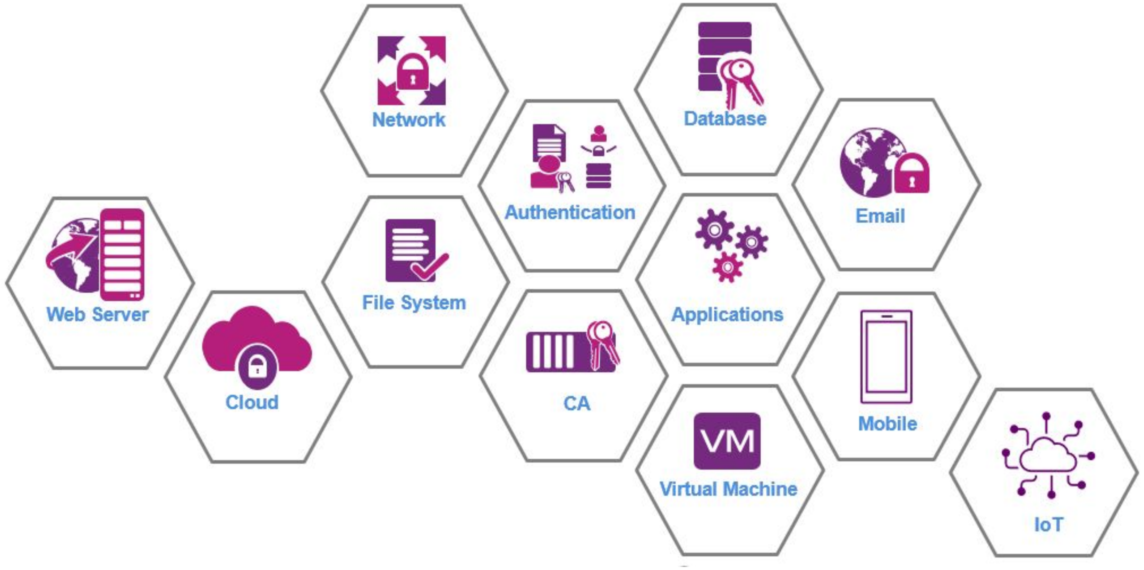
Standards migration

Compliance

Good engineering

Why do you care?

Crypto is Everywhere



- Certificates
- Keys
- Secrets
- Crypto Algorithm
- Crypto Library

PKI and crypto ARE critical infrastructure and usage is ever-expanding

Crypto expert resources are scarce and expensive

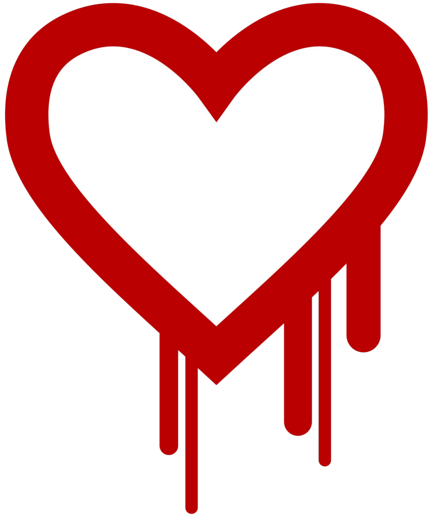
Risks can be unknown because elements are not visible/managed

Many organizations find out too late what it takes to manage crypto assets well

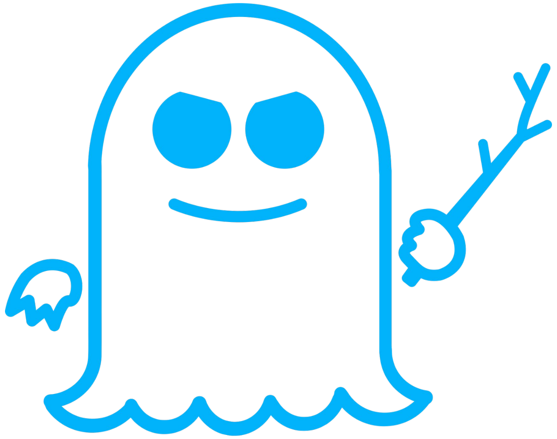
Procedures, Policies and (crypto) platforms are not always robust or maintained

Best practices are **of**ten inconvenient

Implementation Flaws



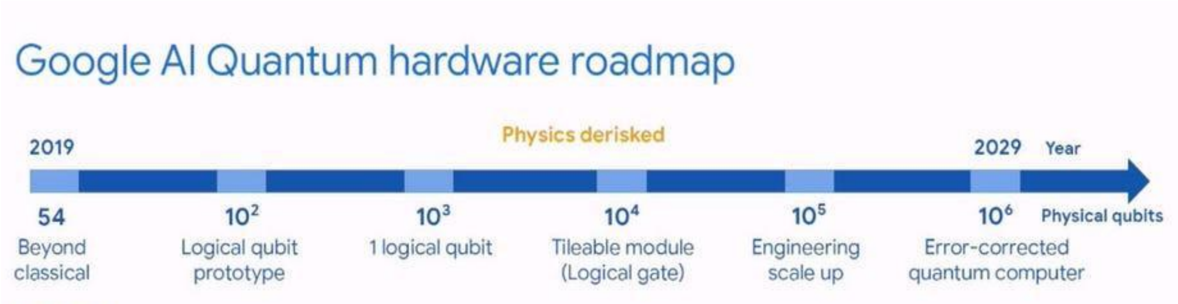
HEARTBLEED



SPECTRE

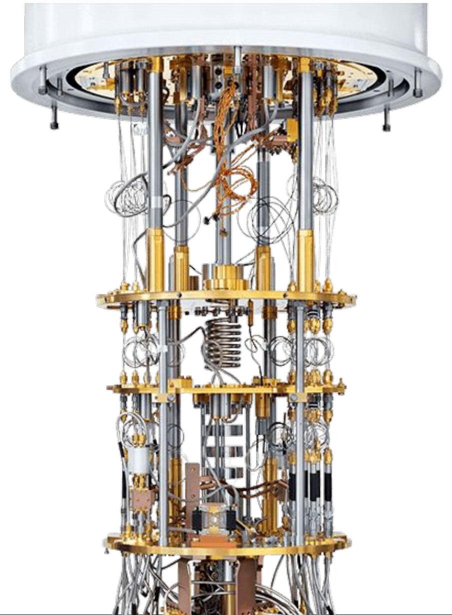
MELTDOWN

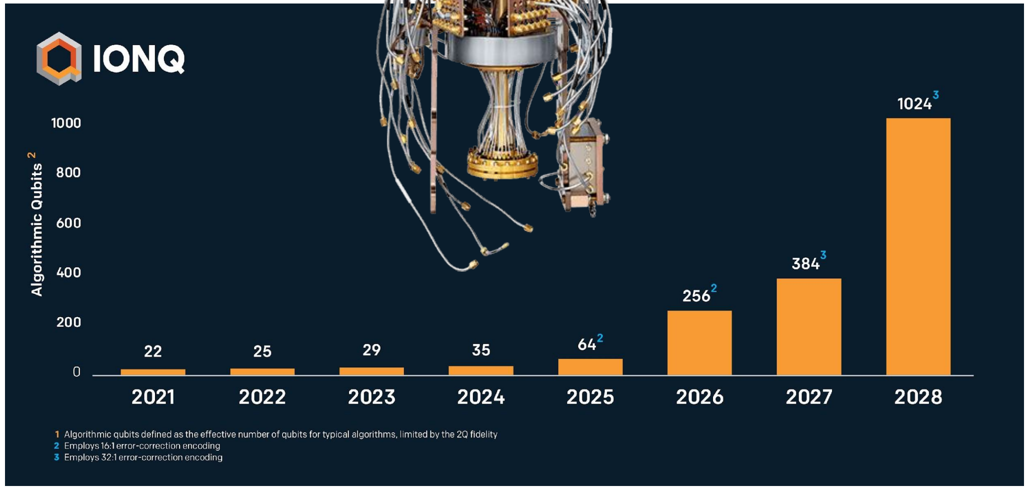
Scaled Quantum Computers are on the Horizon



Google AI Quantum hardware roadmap

Rigetti Aspen-11





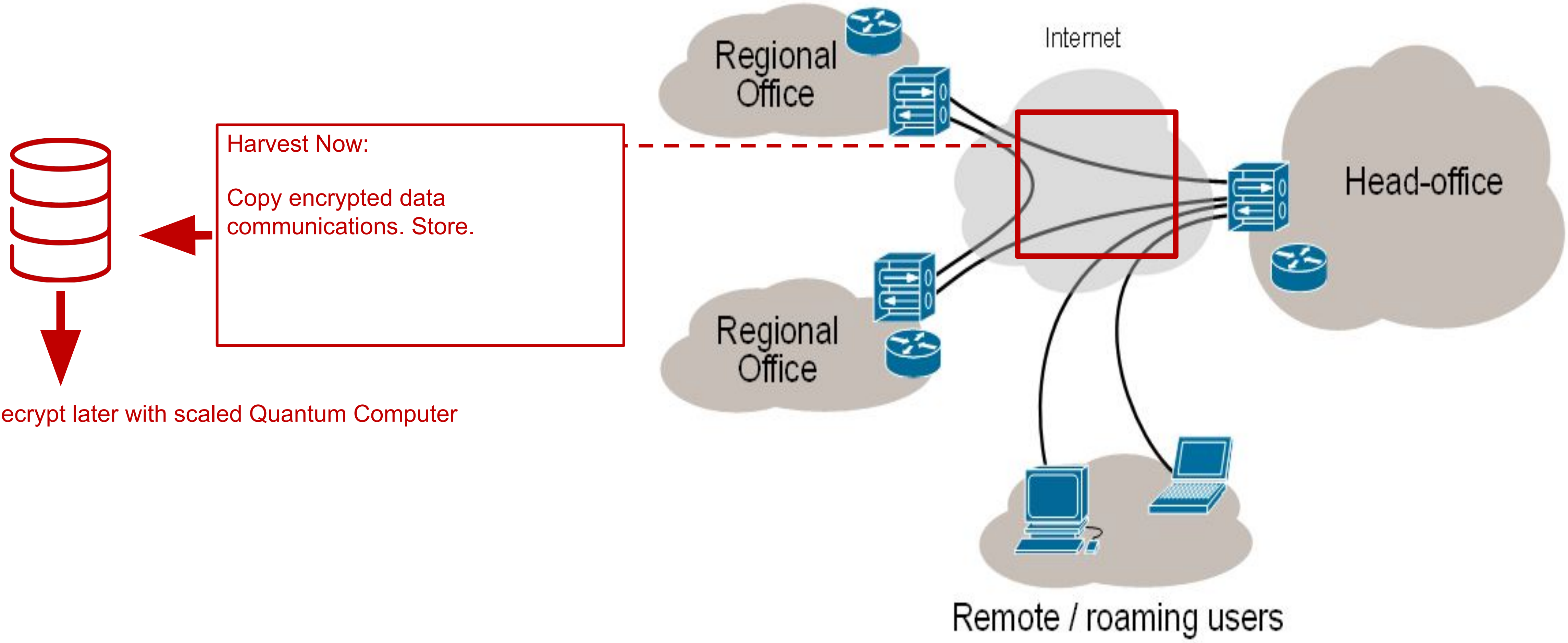
[1] Algorithmic qubits defined as the effective number of qubits for typical algorithms, limited by the 2Q fidelity

[2] Employs 16:1 error-correction encoding

[3] Employs 32:1 error-correction encoding

Harvest Now, Decrypt Later (HNDL)

The Quantum Computing Threat to Long-lived Information Assets



Internet VPN

Harvest Now:

Copy encrypted data communications. Store.

Decrypt later with scaled Quantum Computer

SHE'S HAD YOUR DATA THIS WHOLE TIME
imgflip.com

Post Quantum Cryptography

NIST Standardization

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

Timeline

Apr 2016: NISTIR 8105 Report on PQC

Dec 2016: Call for Proposals

Nov 2017: Deadline for submissions

Apr 2018: 1st NIST PQC Std Workshop

Jan 2019: Round 2 candidates announced

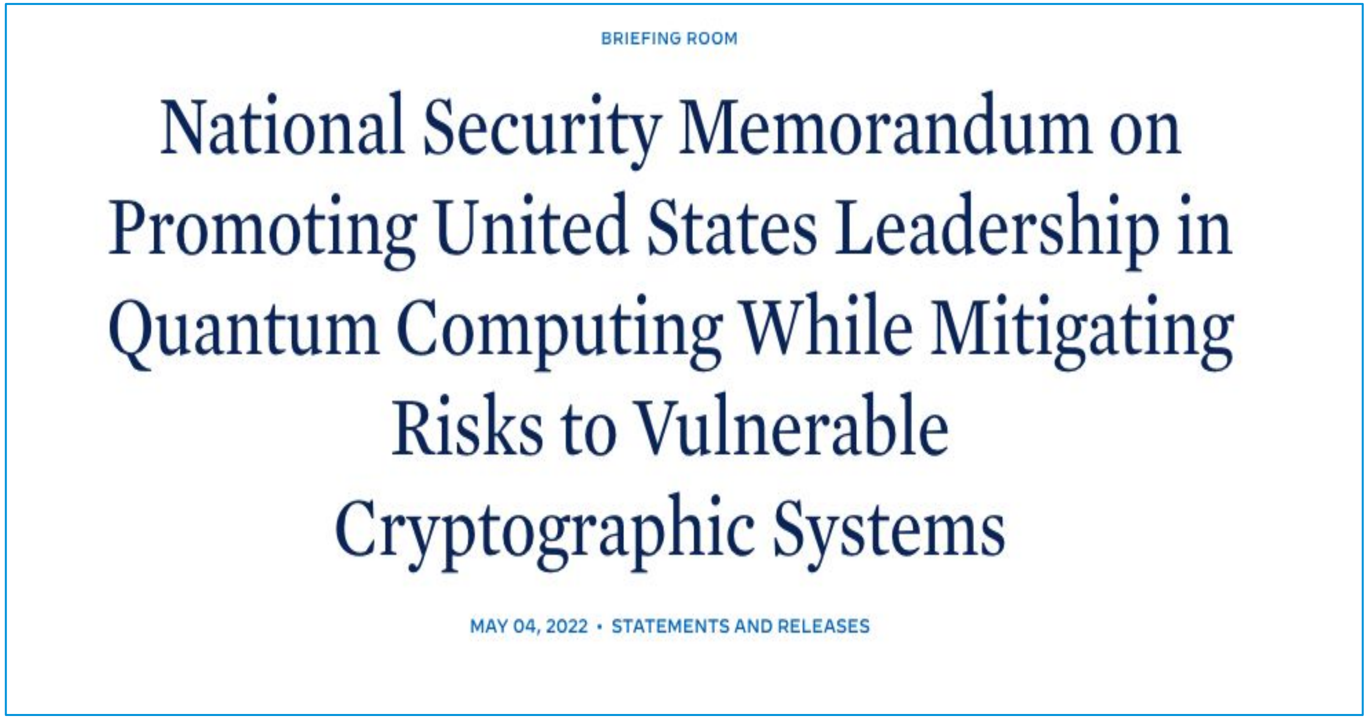
Aug 2019: 2nd NIST PQC Std Workshop

July 2020: Round 3 candidates announced

June 2021: 3rd NIST PQC Std Workshop

July 2022: PQC Draft Standards announced

2024: PQC Standards finalized



BRIEFING ROOM

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

How to prepare?

What can you do now?

Identify crypto libraries in organization

Communicate policies

Identify most valuable assets

Plan and build for change

Create backup plans for CA

What is VMware doing?

Project Newcastle

Project Newcastle

Policy-driven cryptography compliance and configuration platform

- Cryptography Observability
- Define Cryptography Policies
- Automate Reconfiguration
- Support Post Quantum Cryptography
- Audit & Attest Cryptographic Compliance

ChatGPT Jokes

Because Security Can Be Fun

Why did the cryptography algorithm cross the road?

To get to the other side of security and agility!

Why did the encryption system never panic?

Because it had the agility to switch to a stronger algorithm in a crisis!

Why was the crypto system always flexible?

Because it had the agility to change keys at any time!

Why did the encryption algorithm decide to take up yoga?

To improve its crypto agility and be able to bend and stretch to different security requirements!

Please scan the QR Code above to leave feedback on this session