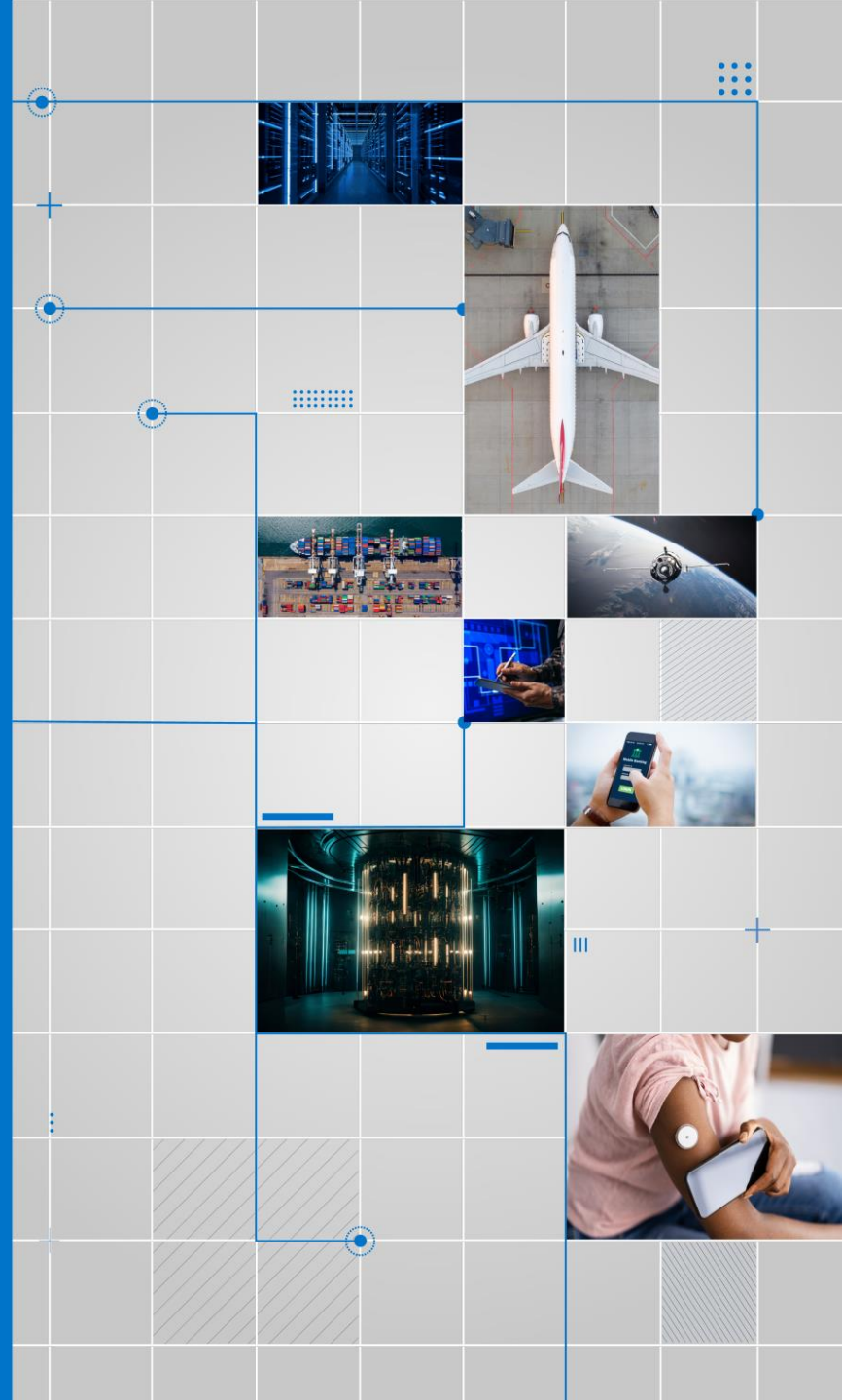
digicert®

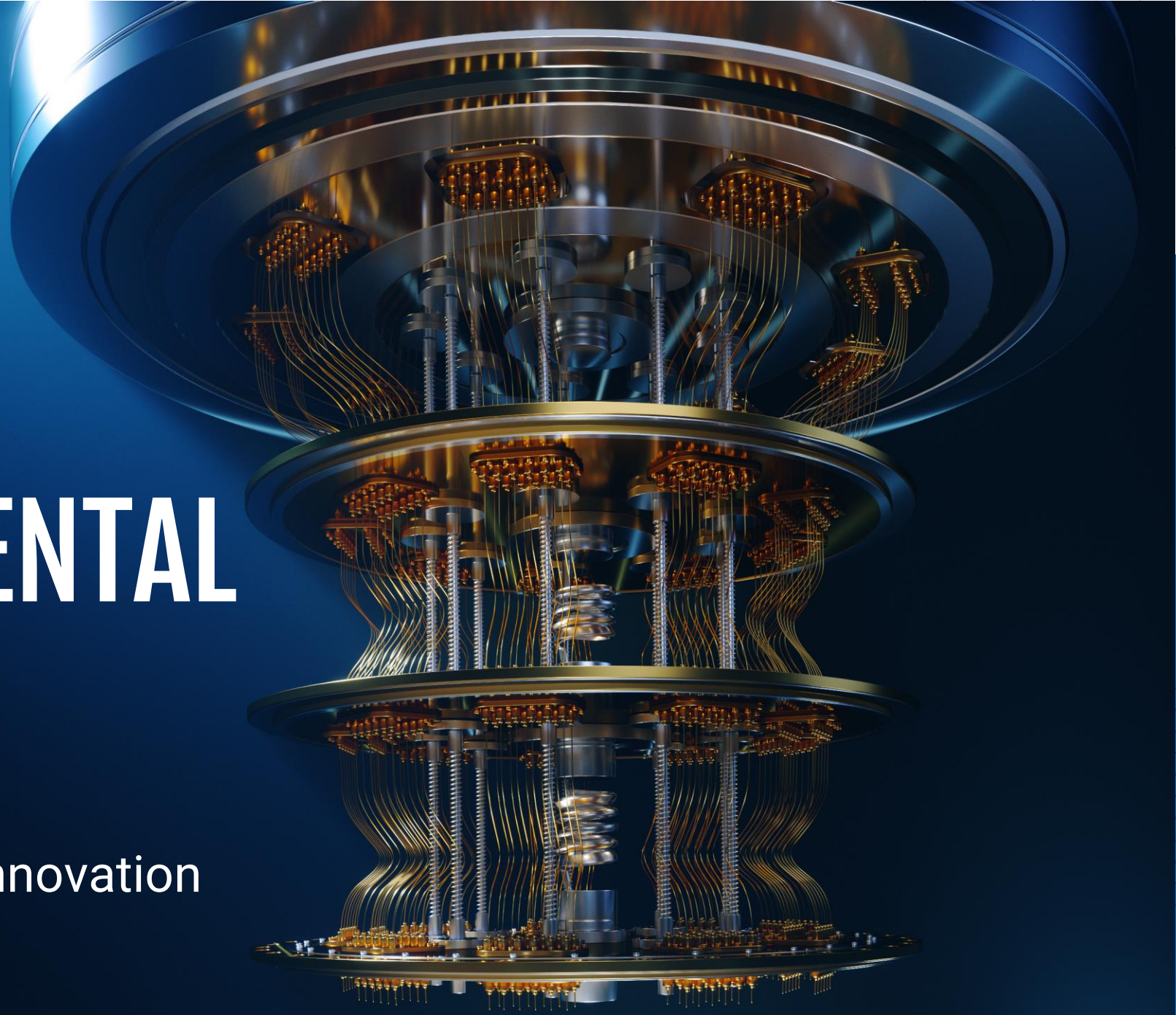
HOW TO PREPARE FOR QUANTUM COMPUTING WITH TODAY'S SOLUTIONS

Daniel Sutherland
Regional VP, ANZ



QUANTUM COMPUTING HAS MONUMENTAL POTENTIAL

1000s of times faster
Accelerate discovery and innovation



THE QUANTUM EFFECT ON TODAY'S CRYPTOGRAPHY

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

THE IMPACT OF QUANTUM COMPUTING

Breaks Security

- Harvest Now; Decrypt Later
- Sensitive Data Exposed
- Encryption Keys Cracked
- Tampered Documents & Software

Upends Business Plans

- Disrupted Supply Chains
- Strategic Plans Unveiled
- Mandatory System Overhauls

Cost & Resource Implications

- Surge in IT Spending
- Training Workforces
- Resource Redistribution

Solution Takes Years

- Not a “drop-in” fix
- Requires architecture changes
- Potential interoperability issues

HOW ARE SECURE COMMUNICATIONS VULNERABLE?

Secure Communication Protocol

Shor's Algorithm breaks current public-key algorithms

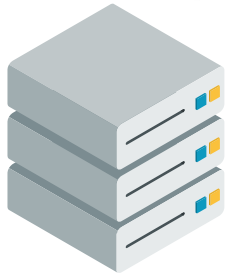
Key Establishment

Authentication

Grover's Algorithm weakens symmetric encryption (square root)

Encrypted Transmissions

A HARVEST & DECRYPT ATTACK ON VPN



VPN Session

Handshake | **Data Exchange**

Quantum attack using Shor's algorithm → **Key Establishment** → Obtain private key → **Ciphertext** → Decrypt using extracted key

QUANTUM RESISTANCE IN THE REAL WORLD

ML-KEM	ML-DSA	SLH-DSA	FN-DSA
Crystals-Kyber	Crystals-Dilithium	SPHINCS+	FALCON
FIPS-203	FIPS-204	FIPS-205	Proposed Name-Released
Key encapsulation for secure communications	Secure identities and electronic signatures	Security for long term use cases	Security for fast transaction processing
Available now from DigiCert	Available now from DigiCert	Available now from DigiCert	Available now from DigiCert

NOW WE HAVE ANOTHER PROBLEM

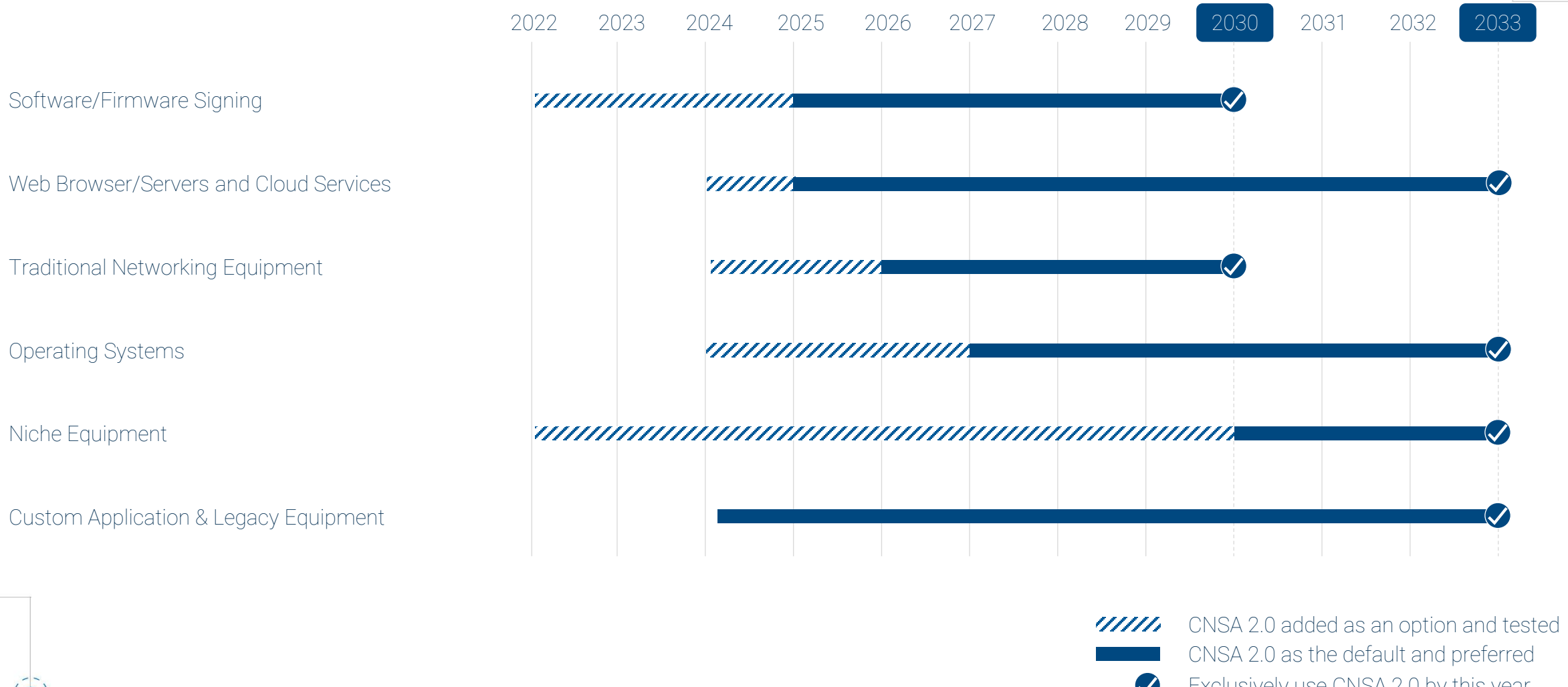
Need to upgrade asymmetric cryptography everywhere that it appears

- Certificates that protect websites
- Certificates that protect email
- Certificates that authenticate users
- Certificates that authenticate devices
- Signatures on signed software
- Signatures on software libraries and components
- Signatures on signed documents
- Revocation services for certificates
- Certificate issuance and management flows
- Security for web services
- Security for mobile applications
- Signatures on LLMs
- Crypto embedded in hardware
- Protocol logic in firewalls
- … and so on

"As certificates expire, RSA needs to retire."

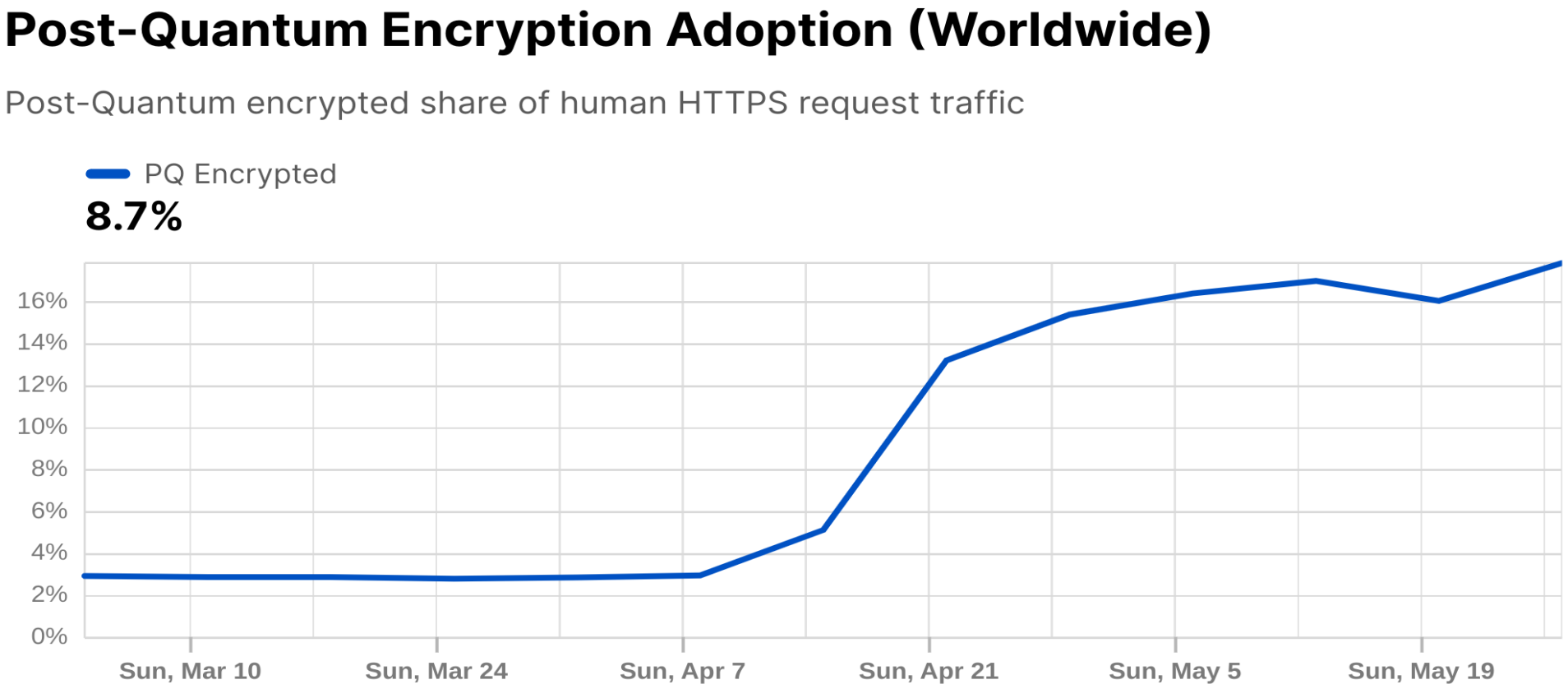
COMMERCIAL TRANSITION TIMELINE

CNSA 2.0 Adoption

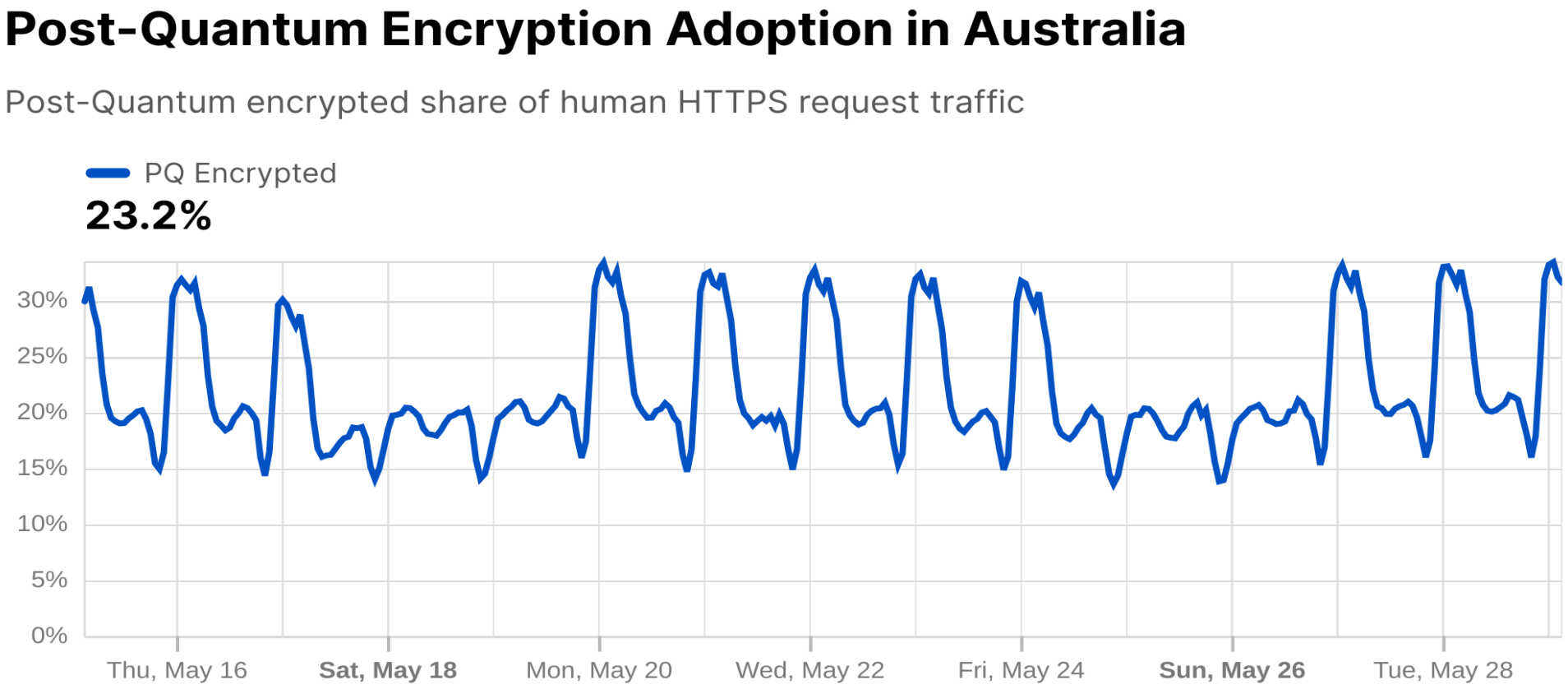


Visual adapted from CNSA *Announcing the Commercial National Security Algorithm Suite 2.0, Figure 1: Transition timeline*

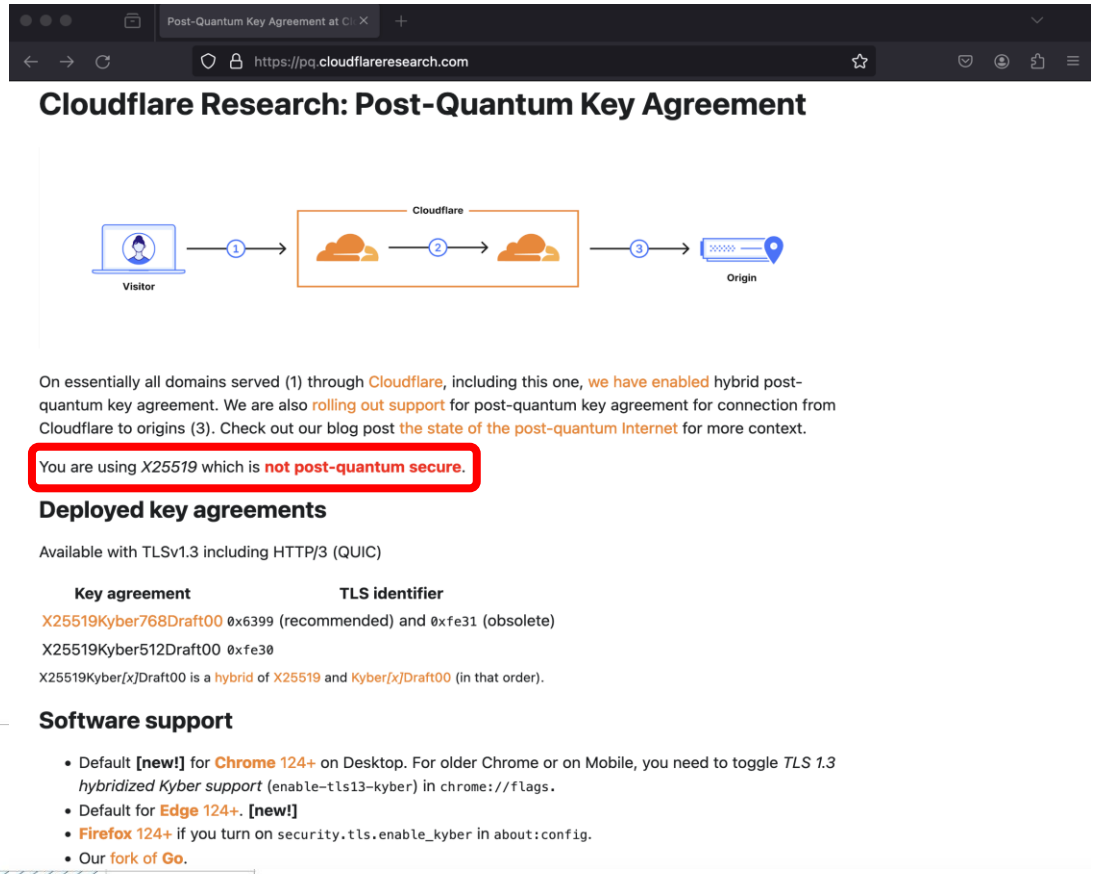
INDUSTRY HAS BEGUN MOVING TOWARDS PQC (3 MONTHS – WORLDWIDE)

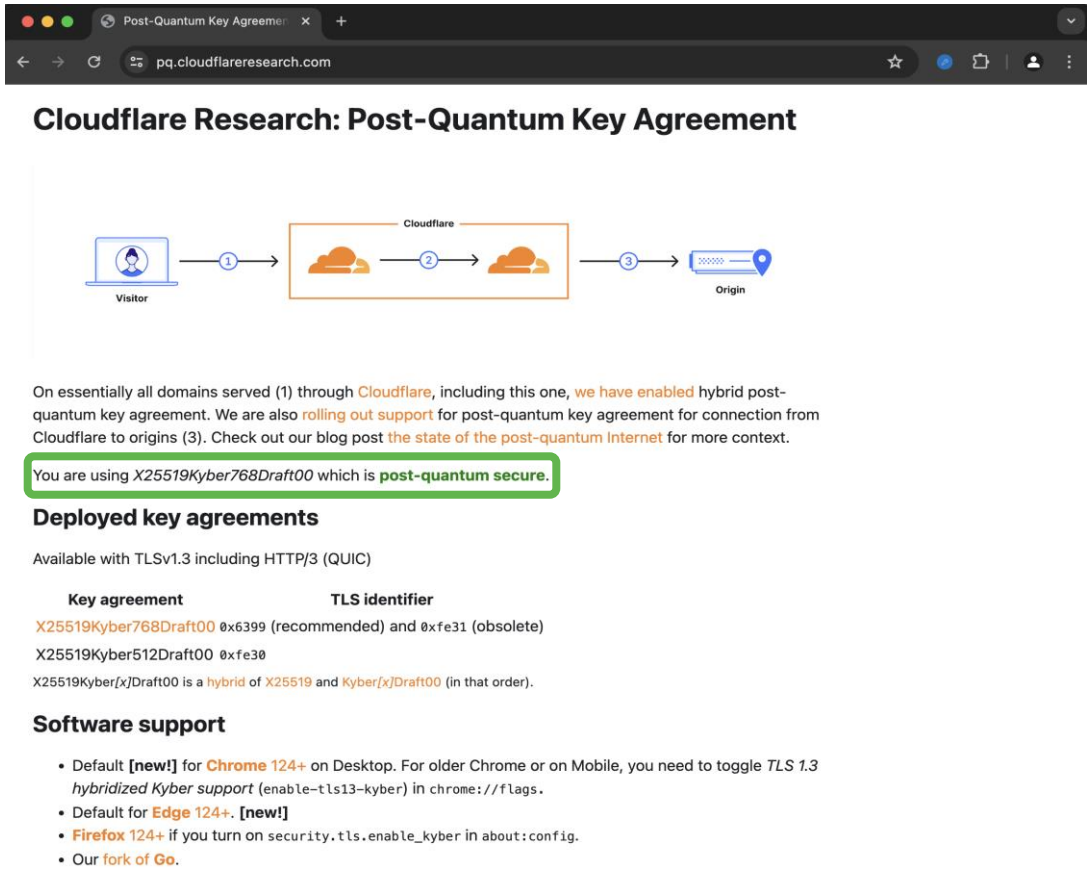


INDUSTRY HAS BEGUN MOVING TOWARDS PQC (2 WEEKS – AUSTRALIA)



ONE BROWSER AT A TIME





A ROAD FULL OF PROBLEMS

Google Chrome's new post-quantum cryptography is causing some issues

News By Craig Hale published yesterday

Chrome 124 not working? Try this

Image credit: Shutterstock (Image credit: Shutterstock)

Cloud Security, Encryption

Chrome users report broken connections after Chrome 124 release

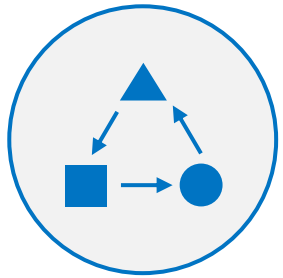
Steve Zurier April 29, 2024

(Adobe Stock Images)

Google Chrome users have been reporting having trouble connecting to websites, servers, and firewalls after Chrome 124 was released last week with quantum-resistant X25519Kyber768 encryption.

THE CHALLENGE

With increased connectivity, the scale of what needs to be updated also increases.



Maintain
Interoperability

Migrate Critical
Systems Faster

Reduce
Switching Costs

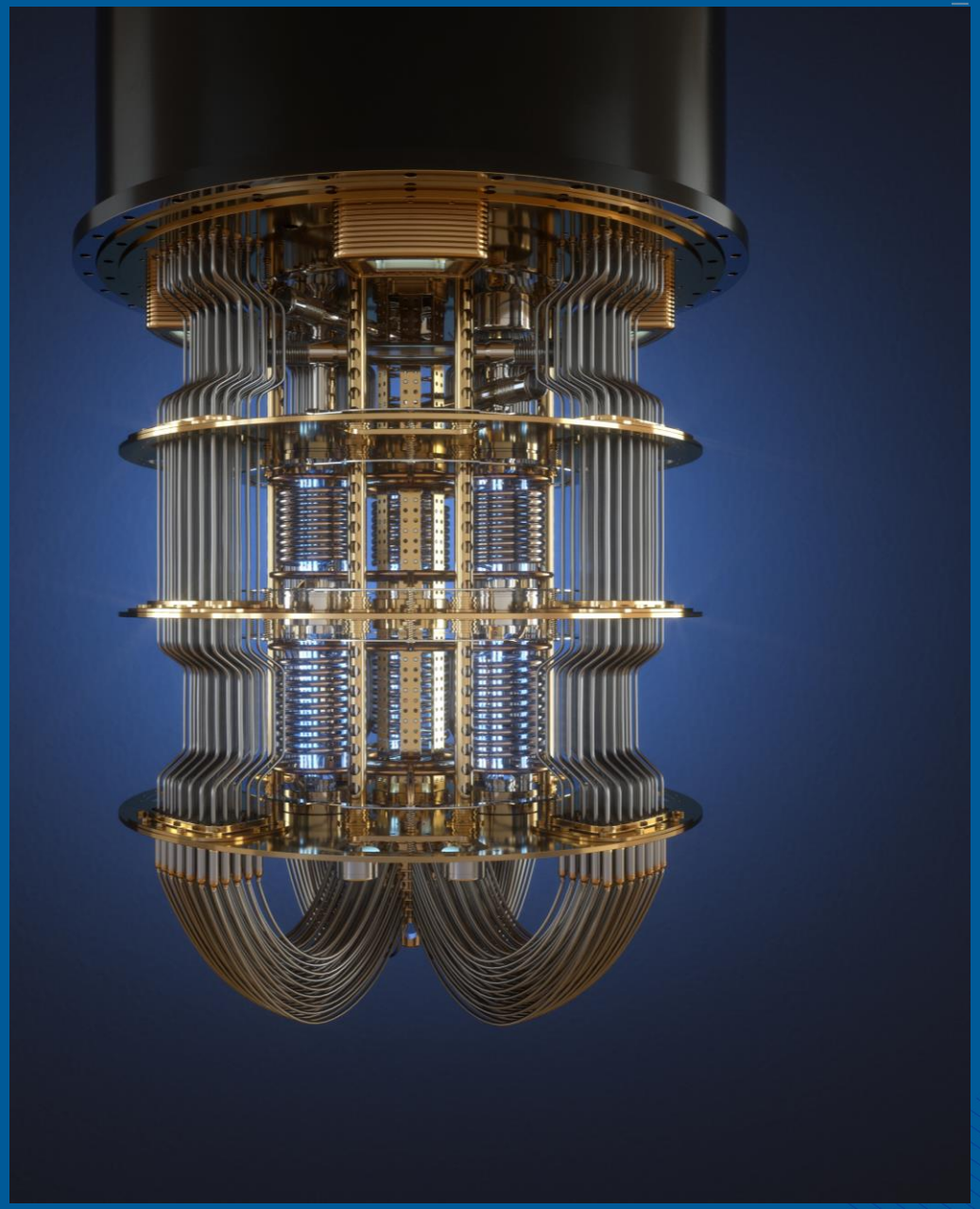
NIST ON CRYPTO AGILITY

"As the replacements for currently standardized public key algorithms are not yet ready, a focus **on maintaining crypto agility is imperative.**

Until new quantum-resistant algorithms are standardized, **agencies should continue to use the recommended algorithms currently specified in NIST standards."**

- "Report on Post-Quantum Cryptography", NIST, April 2016

NIST
National Institute of
Standards and Technology



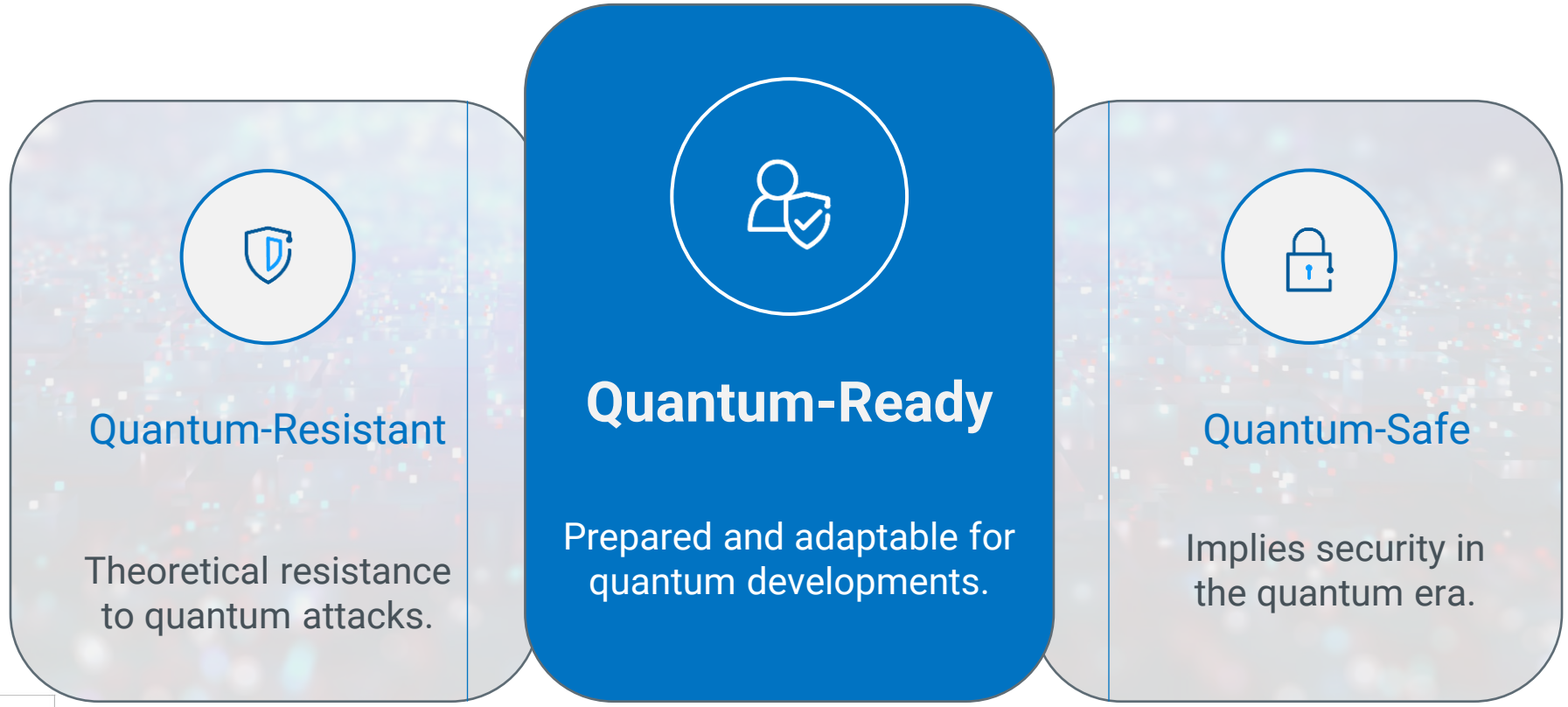
CRYPTO AGILITY – A FRAMEWORK

A design feature that enables updates to future cryptographic algorithms and standards without the need to modify or replace the surrounding infrastructure.

-The US Department of Homeland Security

AGILITY IN UNCERTAINTY

Quantum ready means staying nimble and responsive as quantum technology unfolds.



ROAD TO CRYPTO AGILITY

Discover

Identify and assess quantum vulnerabilities across your digital certificate ecosystem.

Manage

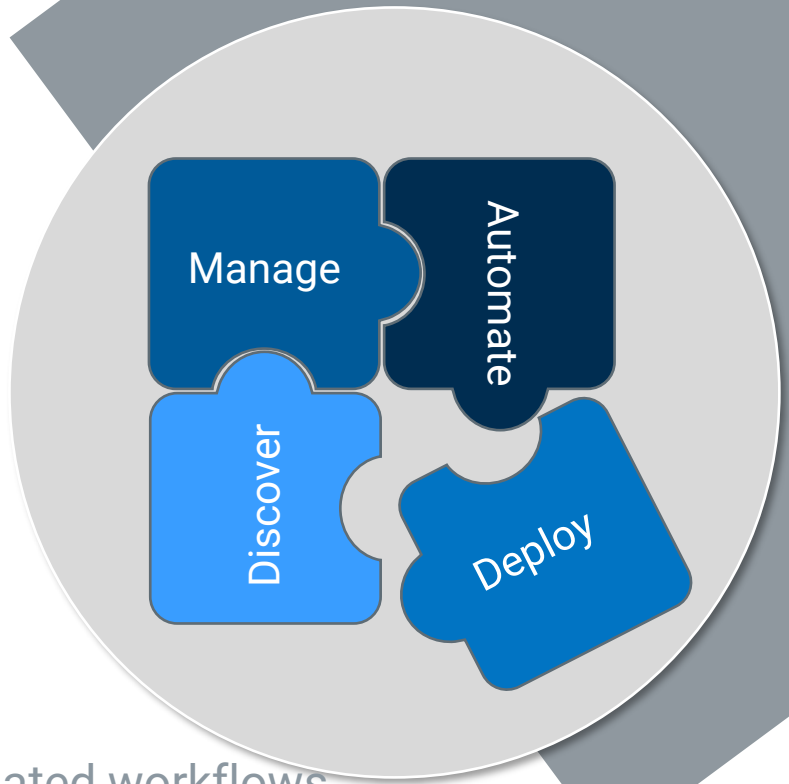
Optimize certificate lifecycle across networks with scalable and automated management tools.

Automate

Facilitate efficient PQC transition through automated workflows, reducing error and operational costs.

Deploy

Enable swift deployment of quantum-safe certificates, ensuring minimal disruption and maximized performance.



DIGICERT'S POSITION

PQC ADVISORY PROGRAM

1

Educate

- Stakeholder Engagement & Training

2

Assess

- Full scope risk Assessment

3

Plan

- Integration & implementation roadmaps

4

Deploy

- Testing and Deployment Best Practices

5

Track

- Future-Proofing Enterprise Systems

DIGICERT PQC PLAYGROUND

Complimentary tools to enable integration, interoperability, and performance testing.
DigiCert experts will help you interpret results to create the right strategic plan.

- Generate certificates to test authentication, digital signatures, key encapsulation
- Understand the integration effort required across your environment
- Identify interoperability risks across internal and external providers
- Measure the computing resources required to support PQC at scale

LABS.DIGICERT.COM

POST-QUANTUM CRYPTO READY PLATFORM

digicert® ONE

ENTERPRISE TRUST	DEVICE TRUST	SOFTWARE TRUST	DOCUMENT TRUST	DNS TRUST
PUBLIC TRUST (CERTCENTRAL)	IOT TRUST MANAGER	SOFTWARE TRUST MANAGER	DOCUMENT TRUST MANAGER	DNS TRUST MANAGER
PRIVATE TRUST	TRUSTCORE			PERFORMANCE MONITORING
CLM & PKI SERVICES (TRUST LIFECYCLE MANAGER)				

Quantum-safe algorithms are the key to future-proof security.

ITU

IETF

ETSI

SAE INTERNATIONAL

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Accredited Standards Committee X9 Inc. Financial Industry Standards

ISO

APPLY WHAT YOU HAVE LEARNED TODAY

Next week you should:

- Conduct your own research on how large-scale quantum computing will impact public-key cryptography and how it will affect your business

In the first three months following this presentation you should:

- Perform an archeological expedition to understand how cryptography is used in your organization
- Identify and prioritize high-value assets for migration

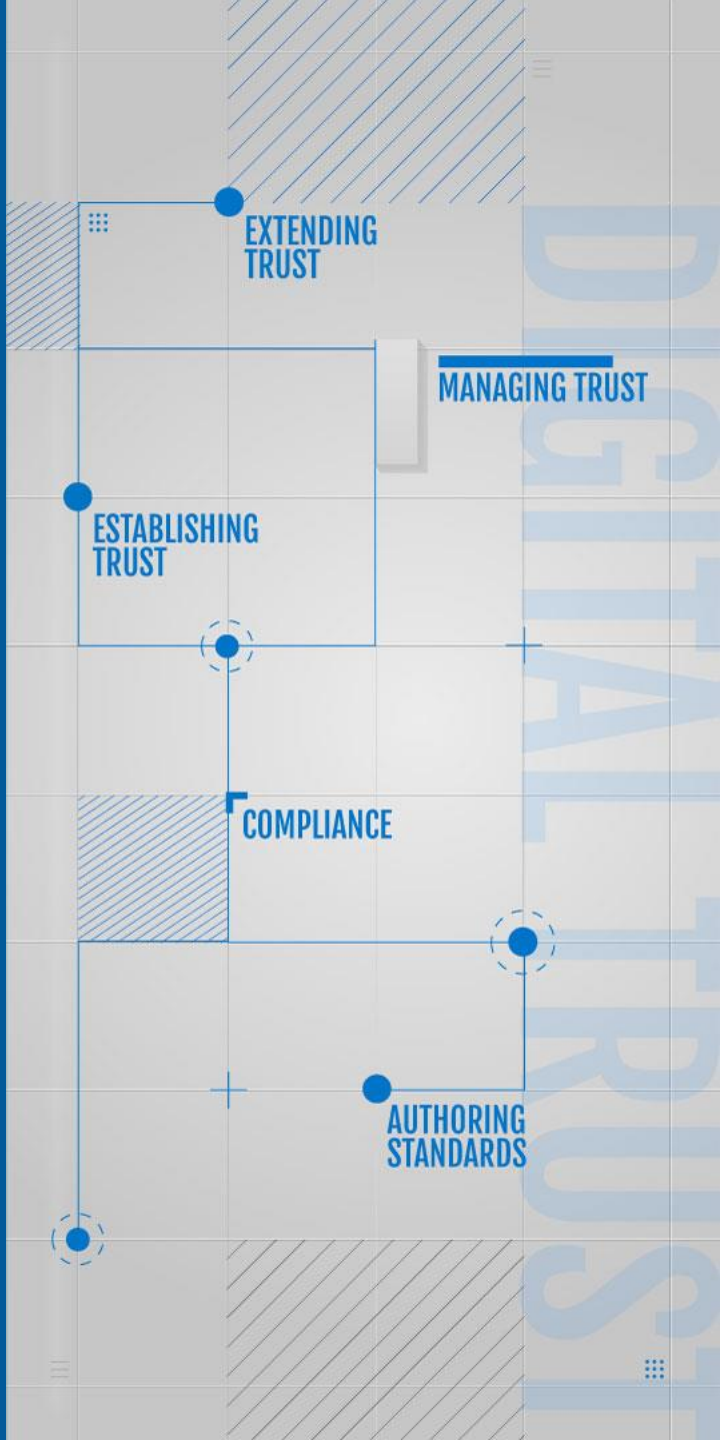
Within six months you should:

- Collaborate with your internal team to create a migration plan
- Share your needs with key vendors to ensure their roadmap aligns

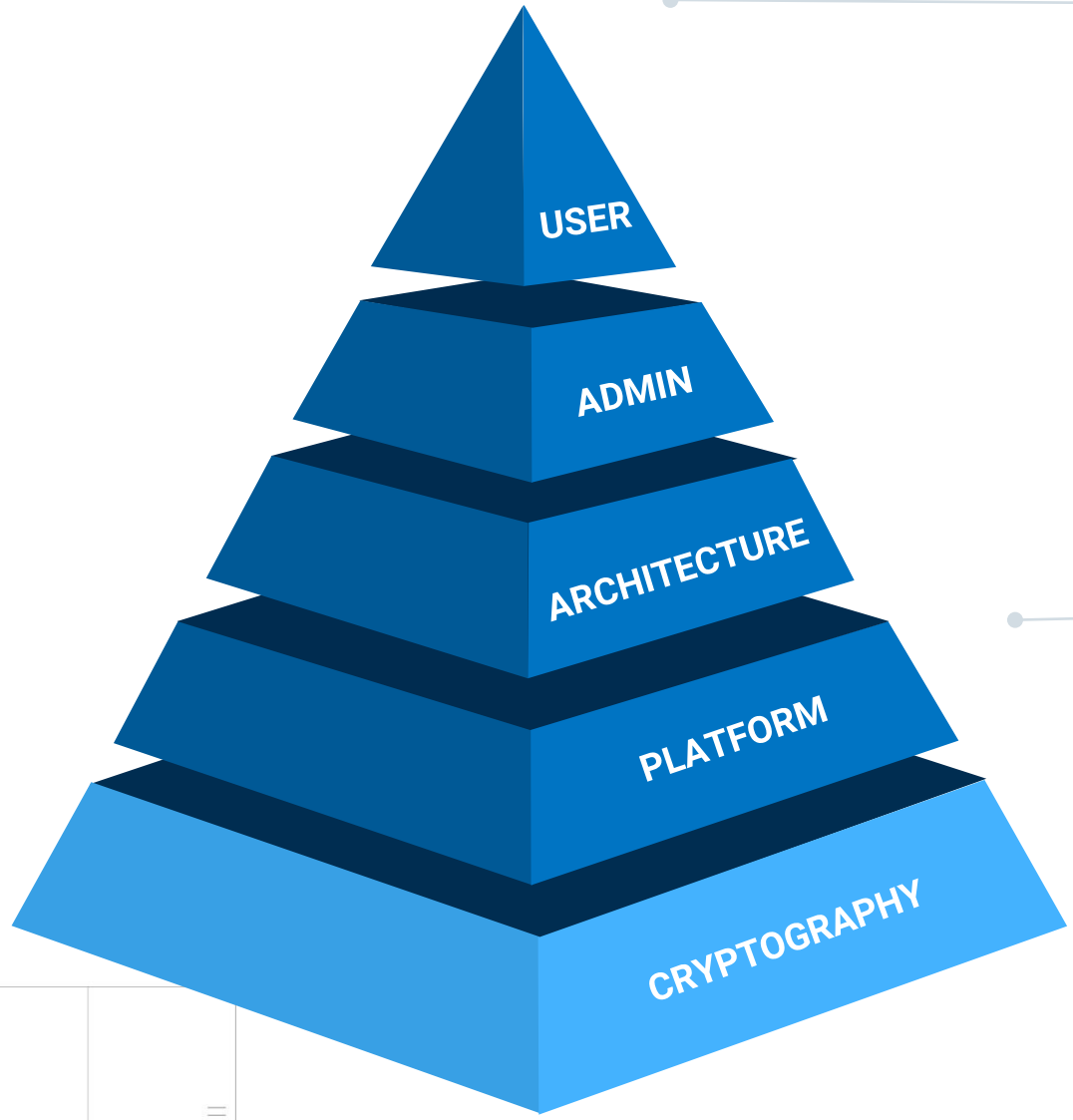
THANK YOU

digicert®

DANIEL.SUTHERLAND@DIGICERT.COM



CRYPTOGRAPHY THE BACKBONE OF EVERYTHING



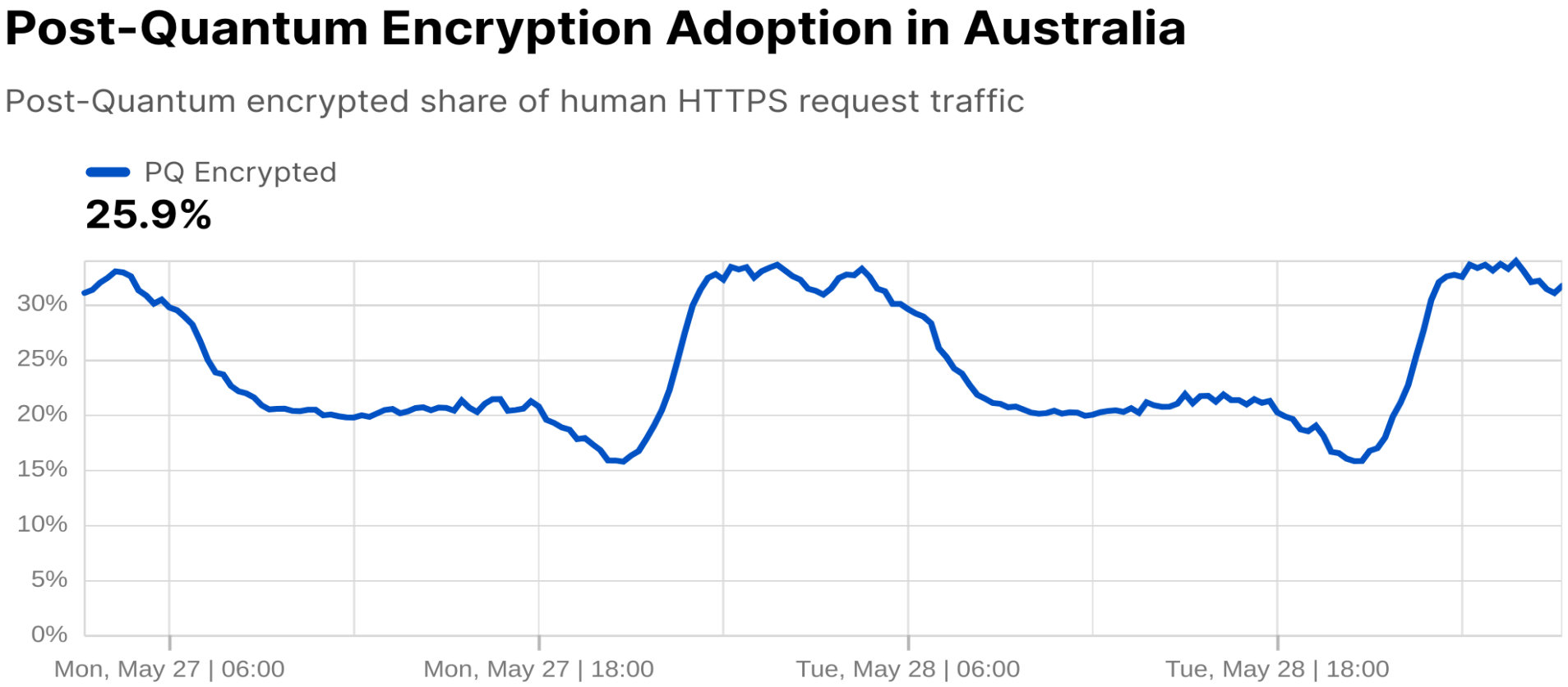
Cause of Security Breaches Today

Quantum: An Unprecedented Threat Looming

MULTIPLE METHODS TO IMPLEMENT PQC SIGNATURES

Hybrid/Catalyst	Chameleons	Composites	Merkle Tree
Extensions modification	Issuance of two certificates	Combining signatures	Storing signatures in CT log
• The alternative key • The alternative signature algorithm • The alternative signature	• A Base certificate • A Delta certificate	• RSA/ECC signature • PQC Signature • Combined Signature	• Offloading of the signature to CT • Depends on CT up time

INDUSTRY HAS BEGUN MOVING TOWARDS PQC (48 HOURS – AUSTRALIA)



THE MIGRATION CHALLENGE

Key Establishment vs. Authentication

Key establishment can be easily upgraded because the client and server negotiate which algorithm to use.

1. Use quantum-safe key transport or key agreement algorithms
2. Use hybrid keys, a mix of both classic and quantum-safe algorithms

The complexity and interconnectivity of public key infrastructure demands action today in order to be ready for the quantum age, and difficult to do while maintaining backward compatibility.