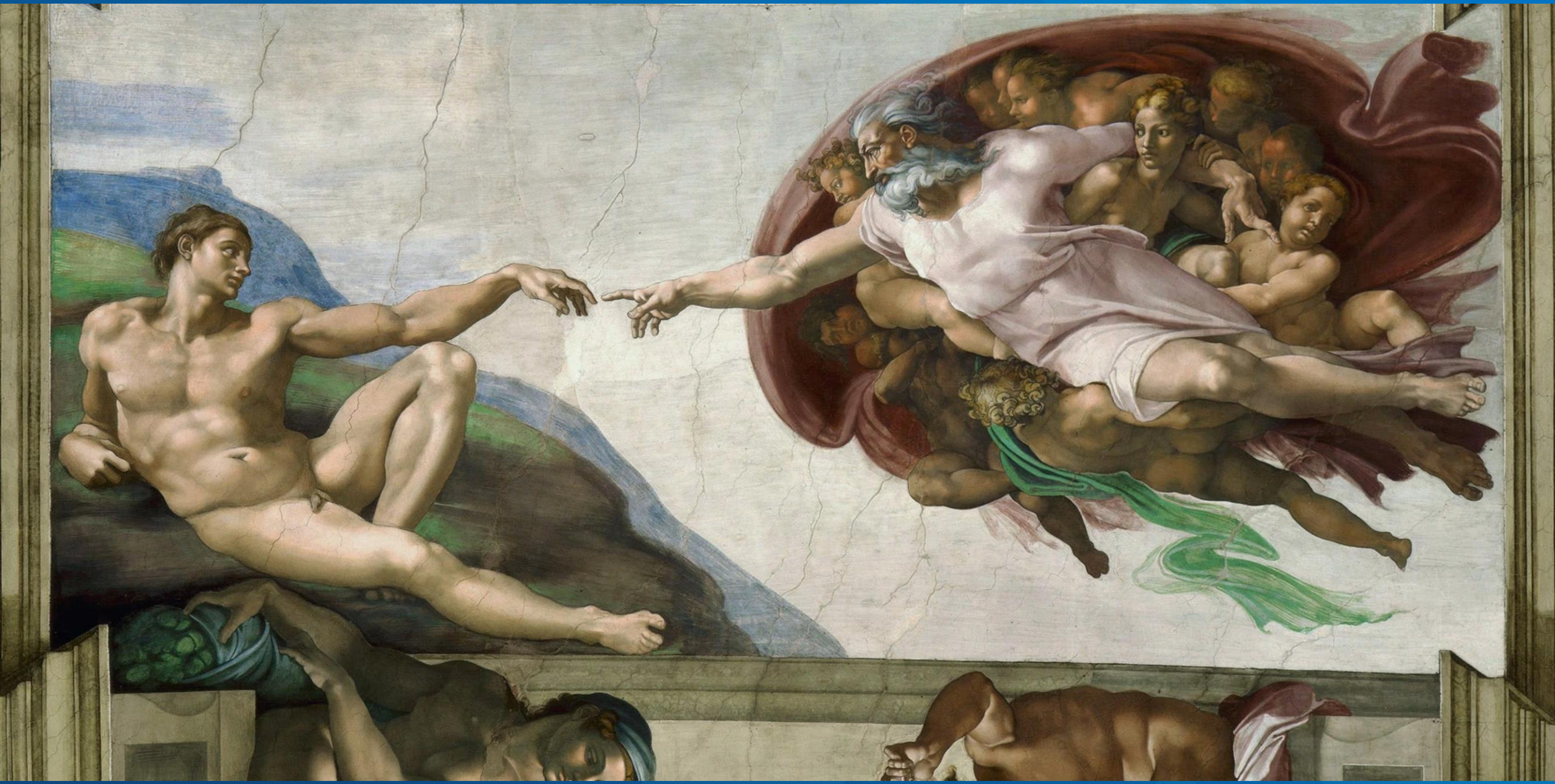
digicert®

# The PKI Renaissance:
## Building Digital Trust for the Modern Enterprise

Daniel Sutherland
Regional Vice President ANZ



# Digital Trust for the Real World



# PKI Complexity Rising Rapidly


**50X**

Machine to User Identities

## Certificate Management is Becoming More Complex

**53%**

Organizations lack sufficient PKI staff

**256K**

Average certificates per organization

Source: Gartner

# Industry Analyst View

PKI is a fundamental building block for **establishing digital trust.**


As certificates continue to gain importance in securing organizations, **effective management of digital trust** becomes imperative.

Gartner®

# Challenge 1: Outages from Expired Certs

MSN

## Google starts rolling out fix for Chromecasts after five-day outage

Good news for annoyed Chromecast owners whose devices haven't been working this week: Google is rolling out a fix for affected devices.

1 week ago

CIO

## ServiceNow certificate error disrupts operations for hundereds of organizations

The expired MID Server Roo G2 SSL certificate caused connectivity failures across multiple services, including Orchestration, Discovery...

Sep 24, 2024


www.thestack.technology

## Expired Certificate crashed $6 trillion Bank of England system

Network configuration, CA and SWIFT issues, and certificate expiration blamed for a series of RTGS outage sthe past year.

Sep 30, 2024

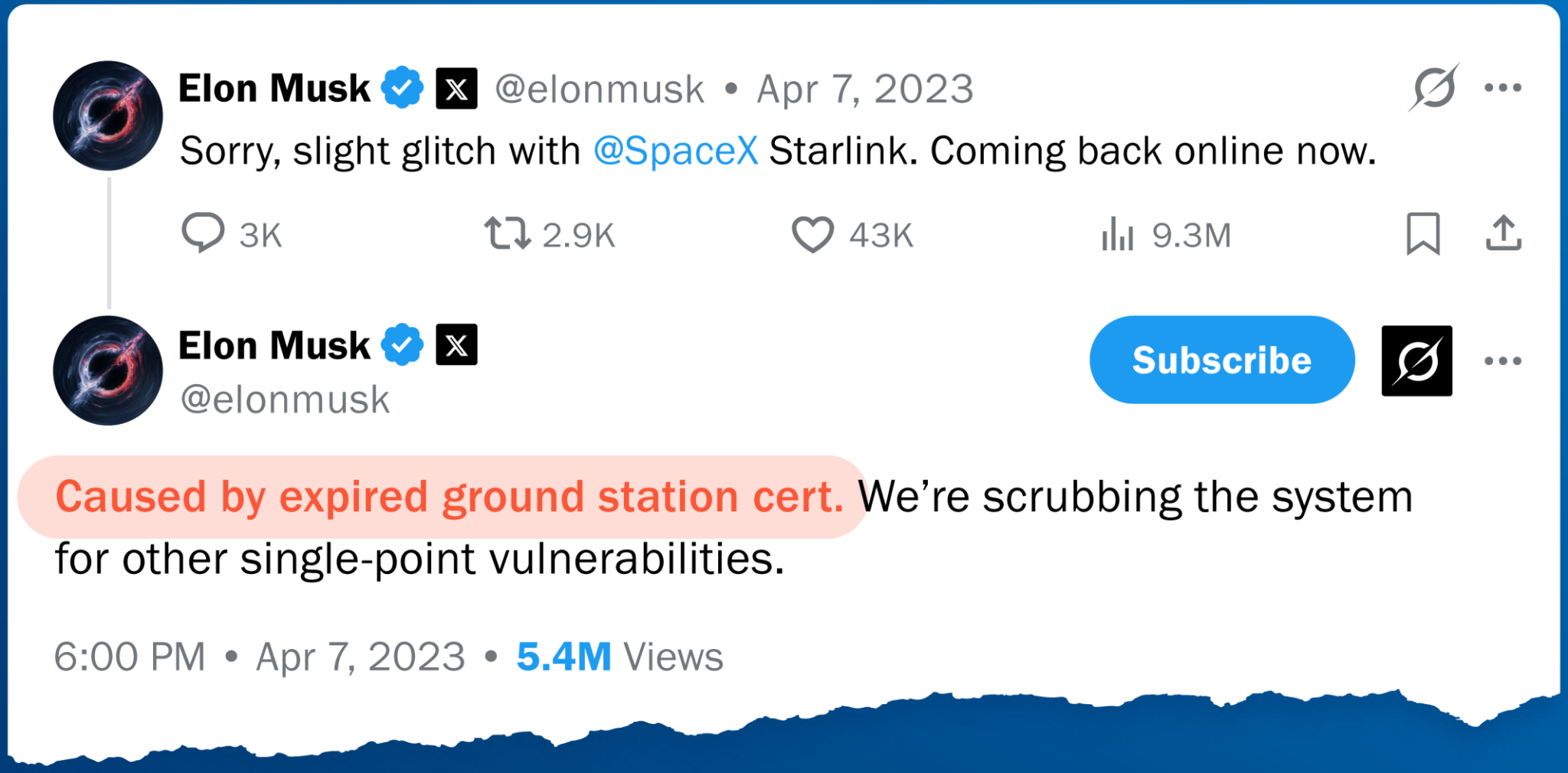
Data Center Knowledge

## Windows Azure Cloud Crashed by Expired SSL Certificate

Microsoft suffered a major outage for its Azure storage cloud and other online services after an SSL certificate expired.

May 30, 2024

# Even Elon Musk is Not Immune...



**Elon Musk** @elonmusk • Apr 7, 2023

Sorry, slight glitch with @SpaceX Starlink. Coming back online now.

3K 2.9K 43K 9.3M

**Elon Musk**
@elonmusk

Subscribe

Caused by expired ground station cert. We're scrubbing the system for other single-point vulnerabilities.

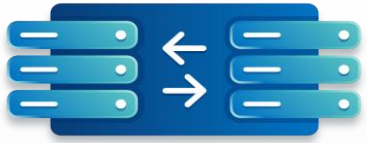
6:00 PM • Apr 7, 2023 • **5.4M** Views

# Challenge 2: Web PKI Changes

## a) Certificate Lifetimes are Shortening

# b) Chrome Root Policy Change Summary

Chrome is moving to reject TLS certificates configured for client authentication



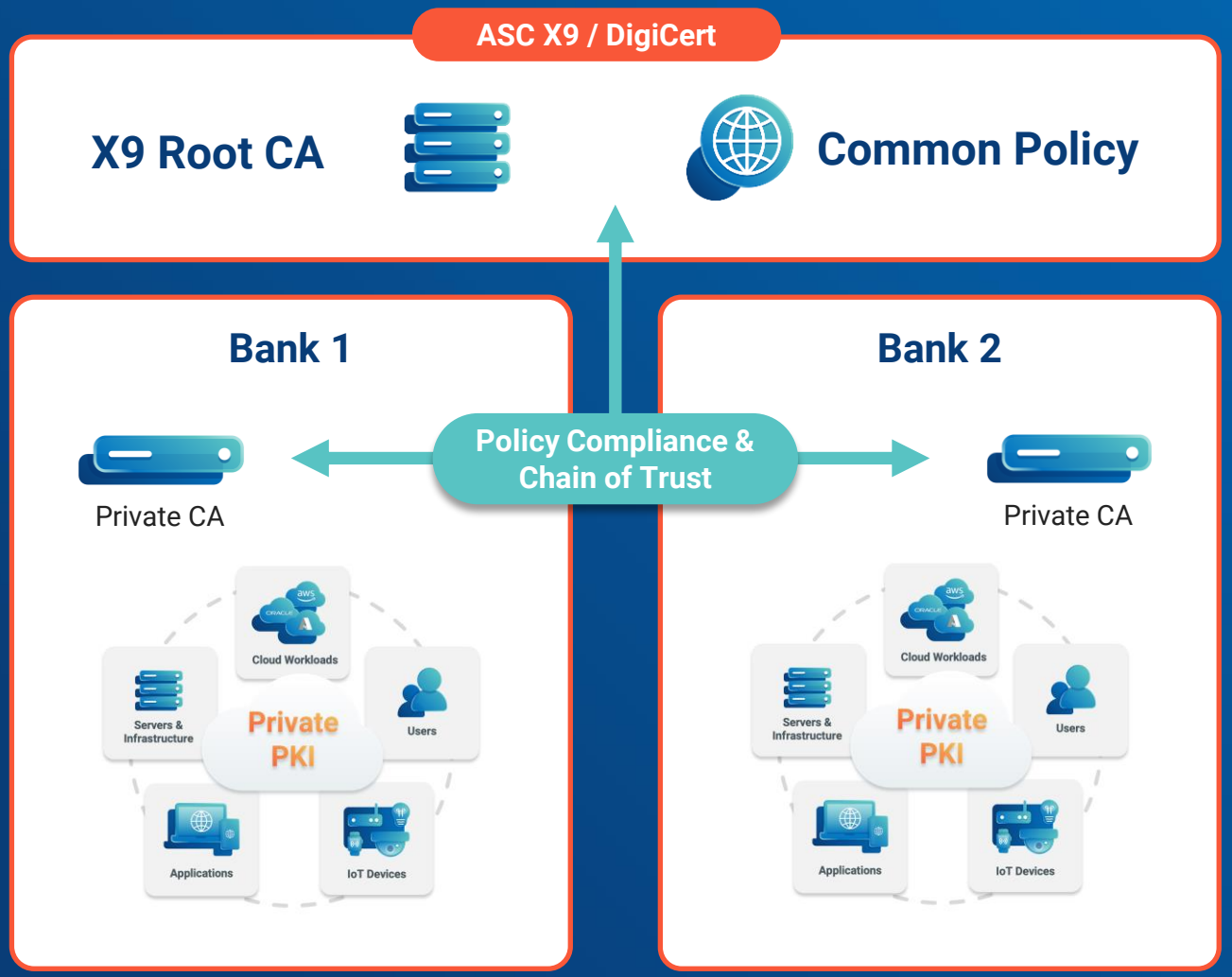
Impacts mTLS communications that use public TLS certificates

Part of push to enforce stricter separation of certificate uses

Public CAs like DigiCert must stop including client authentication setting (EKU) in public TLS certificates

## Chrome Timeline

# X9 PKI: The Best of Public & Private PKI




Consortium-Driven Policy

Trust Across Boundaries

Consistency With Flexibility

Better Security & Compliance

# Challenge 3: Regulatory Compliance


**NIS 2 Directive**
Increased Operators of Essential Services (OES) required to comply by **17 Oct 2024**


**Cybersecurity in Medical Devices Submission Guidance**
Provide a Software Bill of Materials by
**01 October 2023**


**Payment Card Industry DSS**
Inventory & vulnerability management by
**1 April 2025**

**EU Cyber Resilience Act**
Med Device, IoT & ICT Compliant Products by
**2027**


**Digital Operational Resilience Act**
Risk & vulnerability management tools by
**January 2025**

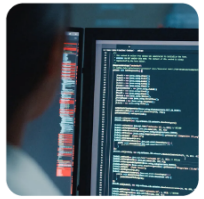
# Challenge 4: Software Supply Chain Integrity

Cybersecurity Dive

## Supply chain attack against GitHub Action triggers massive exposure of secrets

The incident highlights ongoing security concerns in the software supply chain.

1 week ago

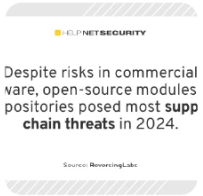


Help Net Security

## Hackers target AI and crypto as software supply chain risks grow

Software supply chain attacks are rising as open-source and commercial software face critical vulnerabilities and targeted threats.

6 days ago



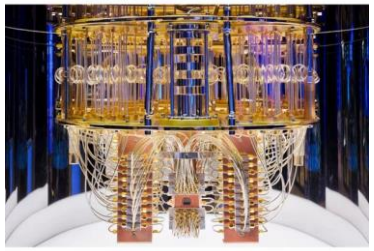

Security Magazine

## Software supply chain experiences almost 1 attack every 2 days

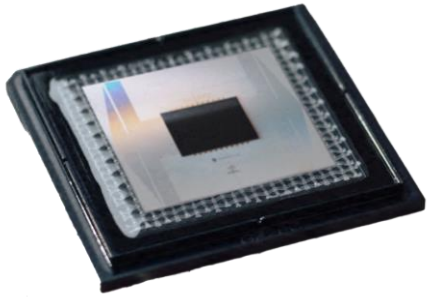
Software supply chain experiences almost 1 attack every 2 days ... In 2024, the software supply chain has faced attacks at a minimum rate of one...

Sep 2, 2024

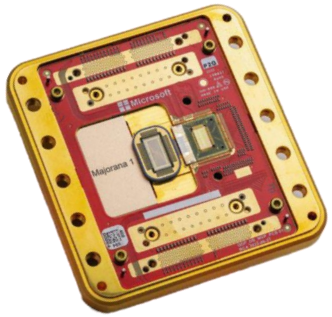
# Challenge 5: Quantum Computing Advancing



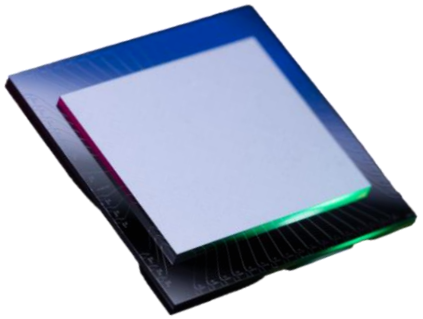
**IBM** Quantum System One
(Mar 2023)



**Google** Willow
(Dec 2024)



**Microsoft** Majorana 1
(Feb 2025)



**Amazon** Ocelot
(Feb 2025)

## Benefits

- Unprecedented compute power
- Drug discovery, climate modelling
- Supply chain and logistics optimization

## Risks

- Breaks current cryptography
- Shor’s algorithm for factoring large numbers
- Grover’s algorithm for search

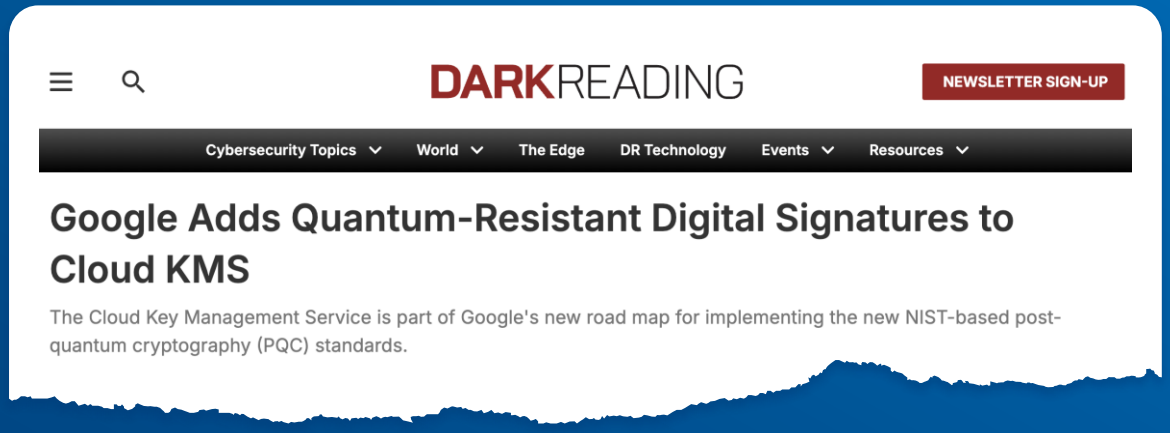
# Post Quantum Cryptography (PQC) is Here

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

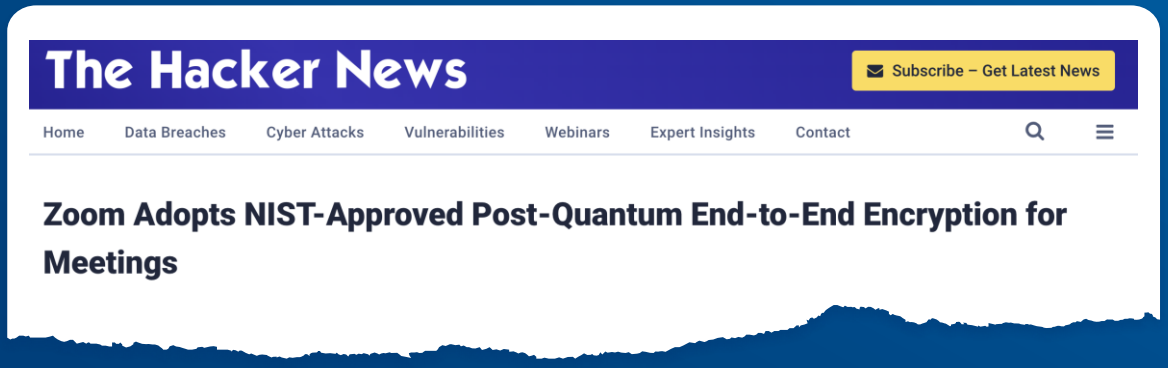
**NIST Released 3 PQC Standards in August, 2024**

| Standard | Purpose | Algorithm |
|---|---|---|
| FIPS 203 | Encryption | **ML-KEM**: Module-Lattice-Based Key-Encapsulation Mechanism (formerly CRYSTALS-Kyber) |
| FIPS 204 | Authentication | **ML-DSA**: Module-Lattice-Based Digital Signature Algorithm (formerly CRYSTALS-Dilithium) |
| FIPS 205 | Authentication | **SLH-DSA**: Stateless Hash-Based Digital Signature Algorithm (formerly SPHINCS+) |

# Industry Leaders are Acting Now








# Transition to Post Quantum Cryptography

## Begin Transitioning to Post-Quantum Cryptography Now

Quantum computing will render traditional cryptography unsafe by 2029. It's worth starting the post-quantum cryptography transition now.

By **Mark Horvath** | September 30, 2024

Gartner

The transition from SHA-1 to SHA-2 took 10 years.

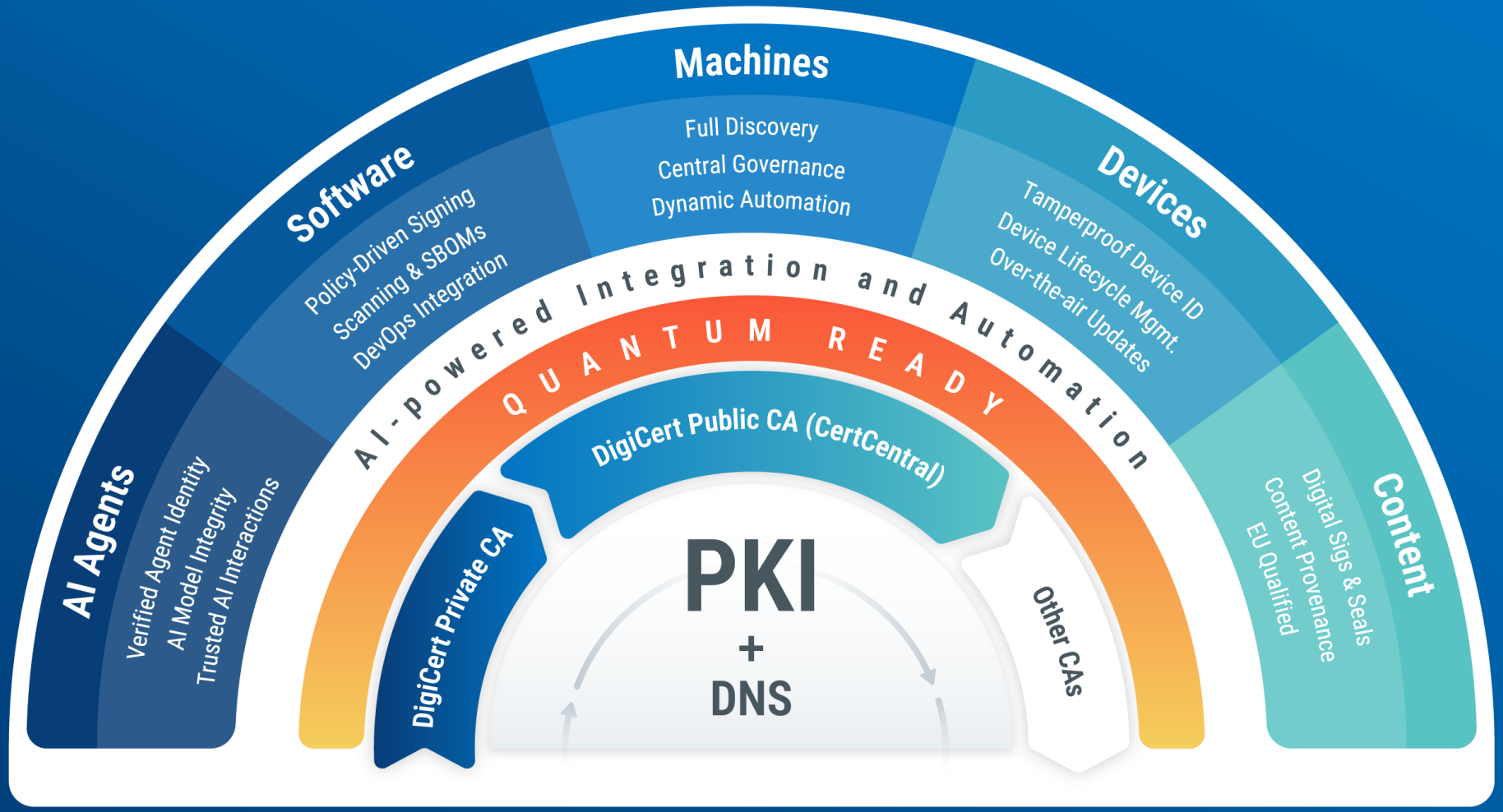
The transition to PQC is a larger, more complex effort.

You will probably only have 3 years to complete it.

Source: https://www.gartner.com/en/articles/post-quantum-cryptography

# Challenges & Opportunities

# The PKI Identity Management Platform




digicert® ONE

# The Modern Digital Trust Ecosystem

digicert®

See us at Booth #40

Daniel.Sutherland@digicert.com

www.digicert.com