Post-Quantum

Cryptography Conference

# How to Sell Post-Quantum Readiness by Combining it with a Zero Trust Journey

**Robert Hann**

Global Vice President of Sales, Cryptographic Center of Excellence at Entrust

ENTRUST HID PKI Consortium

# Making the Connection – Using Zero Trust as the vehicle for PQ Readiness

Robert Hann, VP Digital Center of Excellence

ENTRUST

SECURING A WORLD IN MOTION

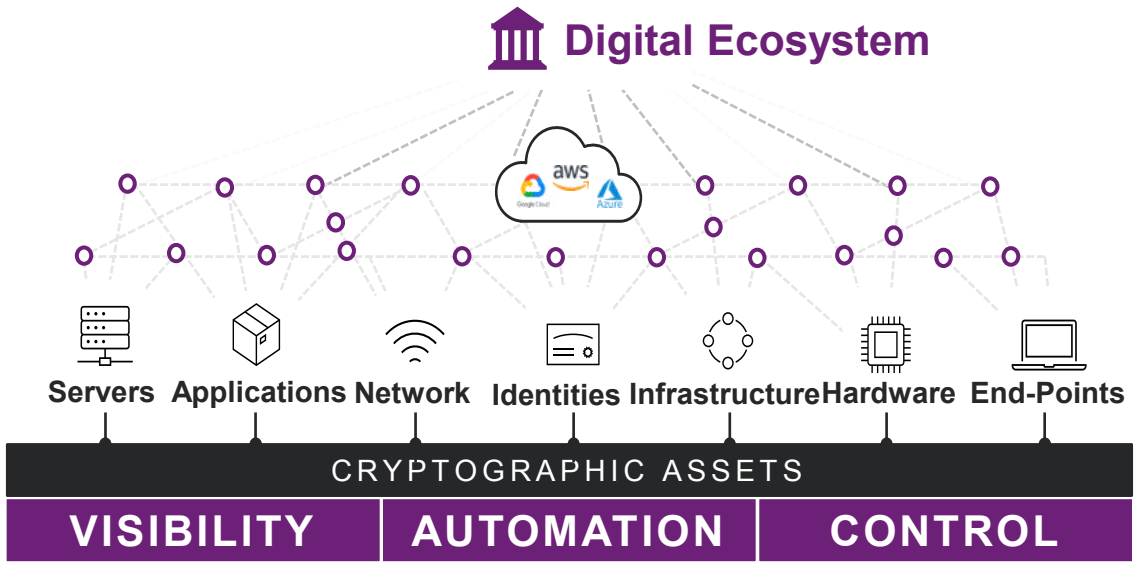
# Agenda

- Managing Cryptography
- Board priorities
- Zero Trust adoption and maturity
- Common journey elements
- Where can PQC help Zero Trust Maturity?
- Recommendations

ENTRUST

# A day in the life of……you!

# Management of Cryptographic Assets




**Problem Statements:**

- PKI and crypto ARE critical infrastructure and expanding
- It is a false assumption that systems are “forever” secured with PKI/crypto
- Risks can be unknown because elements are not visible/managed
- Crypto resources are scarce and expensive
- Best practices are often inconvenient
- Procedures, Policies and platforms are not always robust or maintained
- Many organisations find out too late

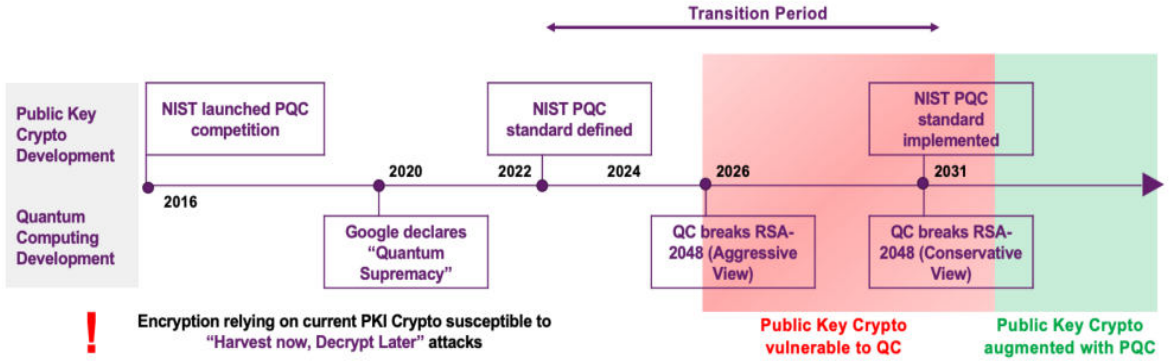
ENTRUST

# The Post Quantum Challenge is Real (but it isn't technical!)

Crypto … is a full time job!

Thank Quantum! At last we will have budget for crypto best practices & PQC migration.

"The time to prepare for PQ is now"….. "yes, we know!"




ENTRUST

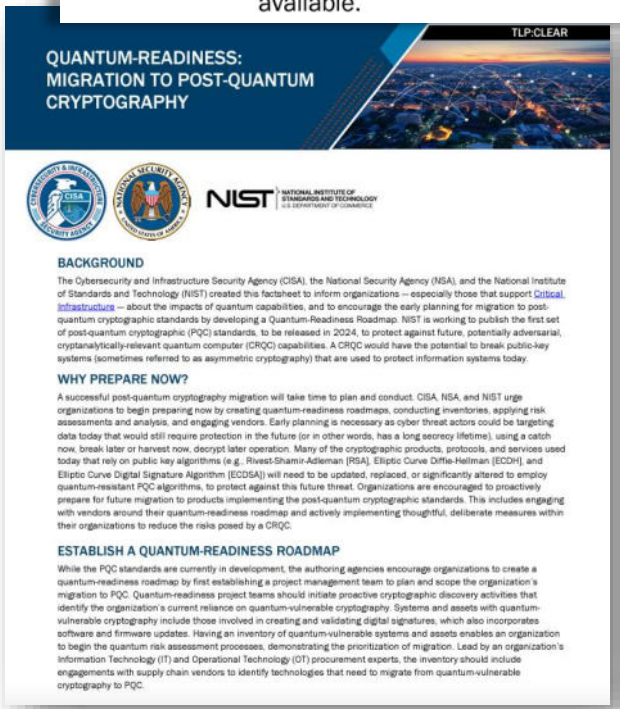
# Board Priorities

## Advantages of a Quantum Computer Running AI

**Quantum computer AI** systems would have a natural advantage over classical computing in many tasks because of their unique ability to apply the principles of quantum mechanics to calculations.

## PREPARE A CRYPTOGRAPHIC INVENTORY

- Having an inventory of quantum-vulnerable technology and associated criticality of the data enables an organization to begin planning for risk assessment processes to prioritize its migration to PQC. This cryptographic inventory will:
  - Help an organization become quantum-ready — a state where a CRQC is not a threat,
  - Help an organization prepare a transition to zero trust architecture,
  - Help identify or correlate outside access to datasets, as those are more exposed and at higher risk, and
  - Inform future analysis by identifying what data may be targeted now and decrypted when a CRQC is available.



TLP:CLEAR

QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

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

**BACKGROUND**

The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) created this factsheet to inform organizations — especially those that support Critical Infrastructure — about the impacts of quantum capabilities, and to encourage the early planning for migration to post-quantum cryptographic standards by developing a Quantum-Readiness Roadmap. NIST is working to publish the first set of post-quantum cryptographic (PQC) standards, to be released in 2024, to protect against future, potentially adversarial, cryptanalytically-relevant quantum computer (CRQC) capabilities. A CRQC would have the potential to break public-key systems (sometimes referred to as asymmetric cryptography) that are used to protect information systems today.

**WHY PREPARE NOW?**

A successful post-quantum cryptography migration will take time to plan and conduct. CISA, NSA, and NIST urge organizations to begin preparing now by creating quantum-readiness roadmaps, conducting inventories, applying risk assessments and analysis, and engaging vendors. Early planning is necessary as cyber threat actors could be targeting data today that would still require protection in the future (or in other words, has a long secrecy lifetime), using a catch now, break later or harvest now, decrypt later operation. Many of the cryptographic products, protocols, and services used today that rely on public key algorithms (e.g., Rivest-Shamir-Adleman [RSA], Elliptic Curve Diffie-Hellman [ECDH], and Elliptic Curve Digital Signature Algorithm [ECDSA]) will need to be updated, replaced, or significantly altered to employ quantum-resistant PQC algorithms, to protect against this future threat. Organizations are encouraged to proactively prepare for future migration to products implementing the post-quantum cryptographic standards. This includes engaging with vendors around their quantum-readiness roadmap and actively implementing thoughtful, deliberate measures within their organizations to reduce the risks posed by a CRQC.

**ESTABLISH A QUANTUM-READINESS ROADMAP**

While the PQC standards are currently in development, the authoring agencies encourage organizations to create a quantum-readiness roadmap by first establishing a project management team to plan and scope the organization's migration to PQC. Quantum-readiness project teams should initiate proactive cryptographic discovery activities that identify the organization's current reliance on quantum-vulnerable cryptography. Systems and assets with quantum-vulnerable cryptography include those involved in creating and validating digital signatures, which also incorporates software and firmware updates. Having an inventory of quantum-vulnerable systems and assets enables an organization to begin the quantum risk assessment processes, demonstrating the prioritization of migration. Lead by an organization's Information Technology (IT) and Operational Technology (OT) procurement experts, the inventory should include engagements with supply chain vendors to identify technologies that need to migrate from quantum-vulnerable cryptography to PQC.


FORBES > FORBES DIGITAL ASSETS

WEB3

## Technologists Are The New Superheroes On Corporate Boards In The Age Of AI, Blockchain And CyberSecurity


ENTRUST

# Zero Trust Strategy

# the STAKES are HIGH

Breaches caused by credential compromise

## NEARLY DOUBLED

over past three years

**61%**
**2022**

**33%**
**2020**

**83%**

of companies had two or more data breaches since 2021

**$4.3M**

Average cost of a breach

ENTRUST

# We are at an inflection point in Cybersecurity

**59%** 59% of organizations have NOT deployed Zero Trust strategies.

**$219B** Cybersecurity spending in 2023.

**$1M** Zero trust can reduce average breach losses by nearly $1M.

**96%** 96% of security decision-makers say Zero Trust is critical to their organization's success.

enisa European Network and Information Security Agency

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


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ENTRUST


10

# What is Zero Trust?
# Enabling a Resilient & Modern Digital Enterprise

"Zero Trust is a **cybersecurity paradigm** focused on resource protection and the premise that **trust is never granted implicitly but must be continually evaluated**."

*- U.S. National Institute of Standards and Technology (NIST)*

Verify Explicitly

Least Privilege

Assume Breach

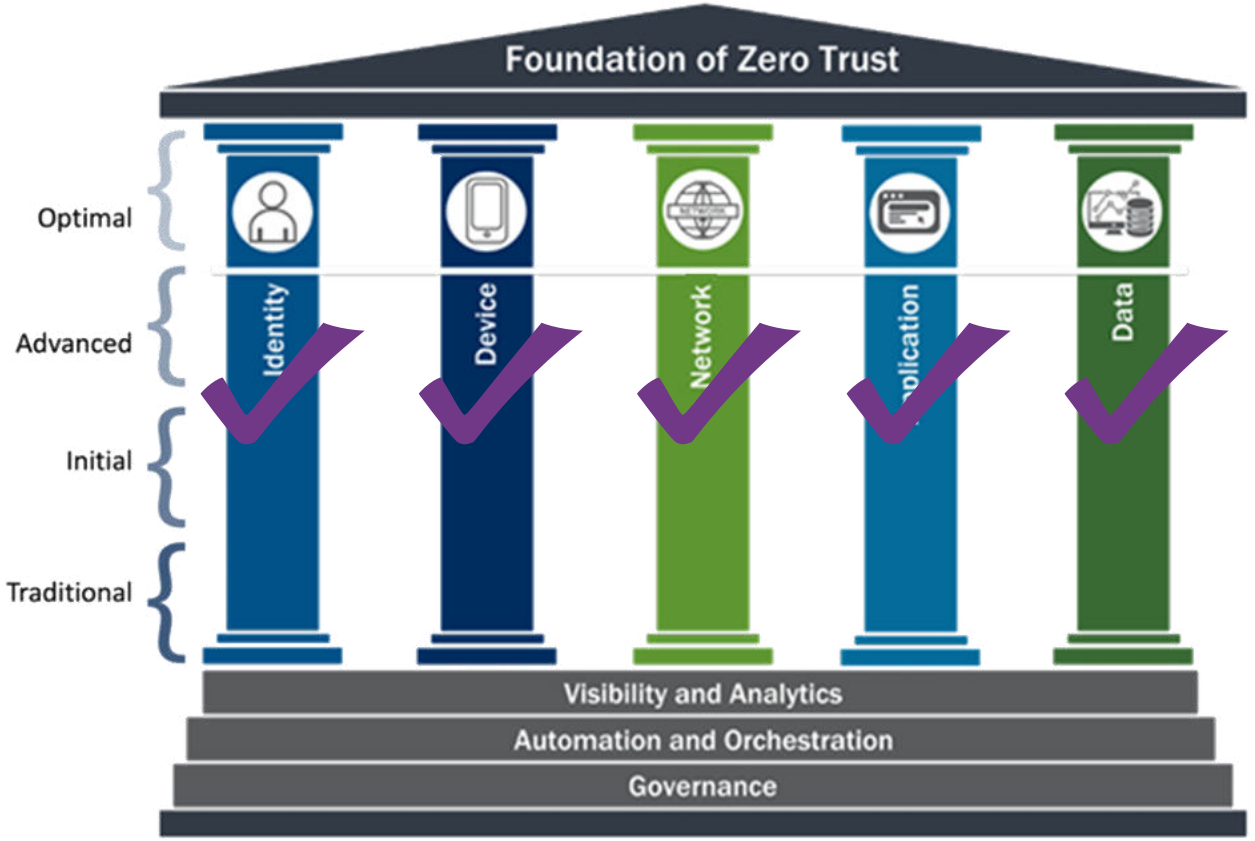
**Never Trust, Always Verify**



ENTRUST

# Establishing a Foundation for Zero Trust

Historically, Zero Trust focused on **networks and identity access** but now it is a comprehensive approach to cybersecurity including **encryption and data security.**




Zero Trust Maturity Model v. 2

*Source: Cybersecurity & Infrastructure Security Agency (CISA)*



ENTRUST

# ~~Post Quantum Zero~~ Trust Journey

**ESTABLISH GROUP**
accountable for

Zero Trust Activity

**INVENTORY CRYPTO ASSETS**
Automated/manual process for keys and

Zero Trust Activity

**MODERNISE & DEFEND**
Simplify, consolidate, replace

Zero Trust Activity

**PQ SECURITY MANAGEMENT**
As the standards, regulations,

Zero Trust Activity

**INVENTORY DATA & FLOWS**

Zero Trust Activity

**CRYPTO AGILITY STRATEGY**
Critical for transition; mitigate risk

Zero Trust Activity

**TEST AND MIGRATE**
With NIST finalist algorithms

Zero Trust Activity



ENTRUST

# PQC, an enabler for Zero Trust

# PQ Readiness Maturing Zero Trust

- PQ Readiness enhances your Zero Trust maturity:
  - Better cyber hygiene through visibility/governance
  - Risk assessment across the full crypto asset inventory
  - Strengthen  ZT Orchestration
  - PQC early to mitigate “Harvest Now – Decrypt Later”
  - PQ/T Hybrid Bridge adds crypto agility

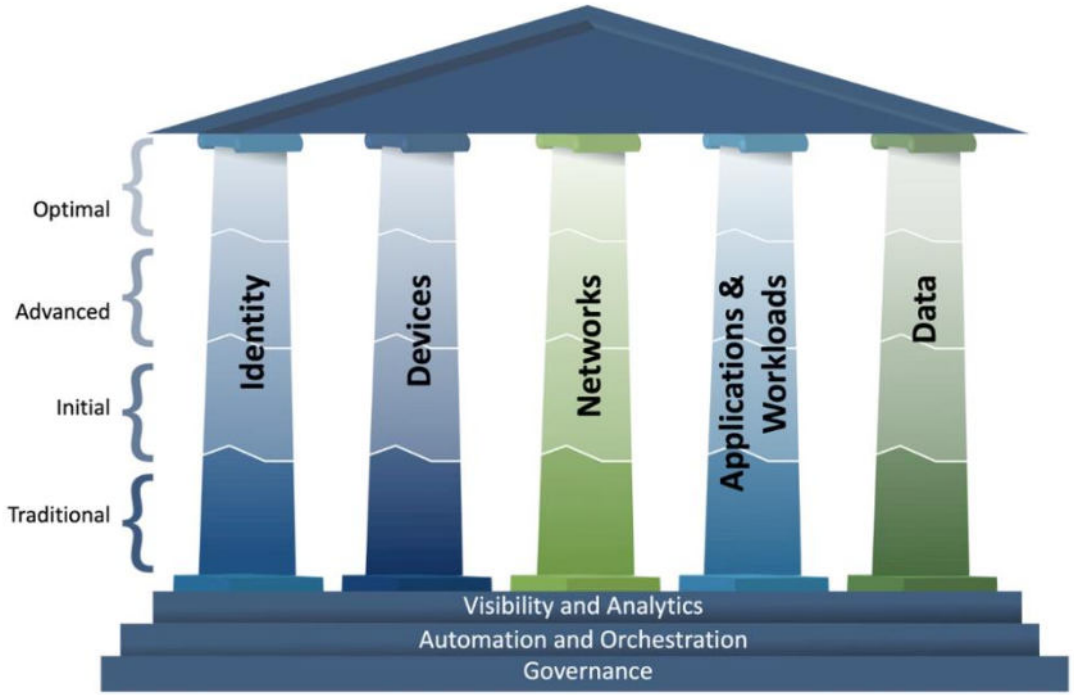



*Figure 3: Zero Trust Maturity Evolution*



ENTRUST

# PQ Readiness for Identity

- Using PQC in Identity and Access Management:
  - PQC in authentication protects against compromised MFA tokens and other elements in access requests
  - PQC certificate based MFA (“phishing resistant”) gives enterprise data increased protection
  - PQC on VPNs and remote desktop services mitigates “Harvest Now-Decrypt Later” threat to your long-term data/contracts



ENTRUST

# PQ Readiness for Devices

- Using PQC in Devices:
  - Strengthens comms/trust between endpoints and management/application services
  - Increased security for sensitive data on endpoints minimizing damage when breached
  - On SIEM systems, protection of log data, comms and other critical components improves security and integrity of monitoring and incident response.
  - Attackers will find it harder to tamper with or evade detection systems



ENTRUST

# Zero Trust for Data, Applications & Workloads


- Using PQC in Data, Applications & Workloads:
  - Encrypting sensitive data at rest and data in transit between applications maintains confidentiality and integrity minimizing unauthorized access.
  - Utilizing PQC for certificate based (Virtual) Machine Identity protects the VM against classical and quantum adversaries.
  - Code Signing with PQC further strengthens the protection of threats like spoofing and maintains the integrity of the trust fabric.



ENTRUST

# Recommendations

- Consolidate the PQ Readiness into your Zero Trust strategy (or even your company AI strategy)
- Elevate/summarize noteworthy Quantum news to Executives
- Tip: Request procurement/security includes PQ Readiness in your supply chain purchasing/assessments

ENTRUST

# Thank You

Questions?

**entrust.com**

© Entrust Corporation

# Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia