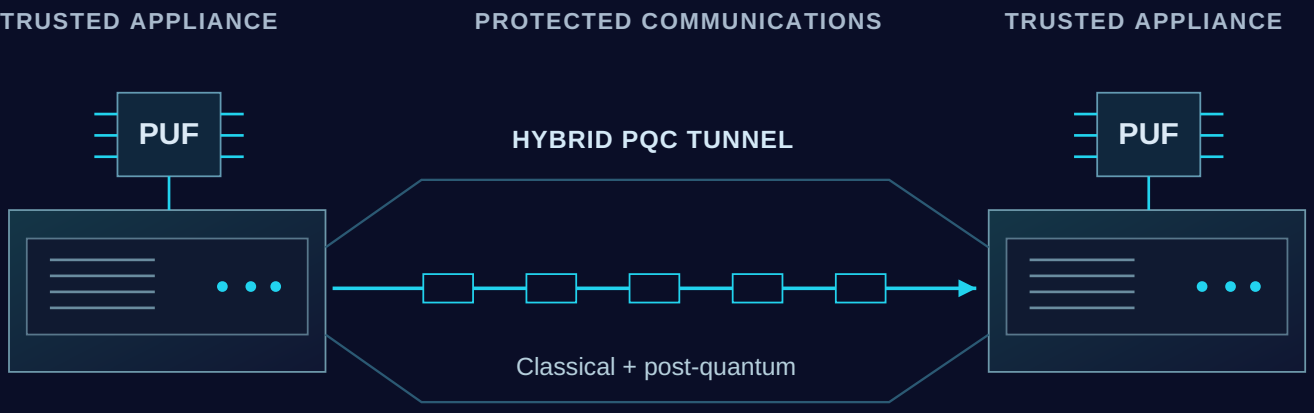
Protect the channel.
Trust the device.

Prepare critical communications for the post-quantum era. Combine a hybrid cryptography migration path with PUF-based hardware identity.

POST-QUANTUM READINESS / PQC & PUF COMMUNICATIONS



Authenticate the device. Bind trust to the appliance.

Preserve interoperability during a phased migration.

Check identity and software integrity.

ARCHITECTURE CAPABILITIES · DEPLOYMENT-SPECIFIC VALIDATION

PQC-ready

A migration path toward quantum-resistant communications

Hybrid

Classical and post-quantum cryptography during transition

Zero Trust

PUF-based hardware identity verification

THE BUSINESS CHALLENGE

Today’s traffic. Tomorrow’s exposure.

Sensitive communications may need to remain confidential for years or decades. Protection applied today must be evaluated against the information’s full lifetime—not only the threat environment at transmission.

Harvest Now, Decrypt Later (HNDL) changes the timing of the risk. An adversary can intercept and archive encrypted traffic now, then wait until quantum capabilities can compromise today’s public-key algorithms.[1–2]

In **2024**, NIST published its first three finalized post-quantum cryptography standards. The historical journey from algorithm standardization to full system integration can take **10–20 years**.[1–2]

Waiting until a cryptographically relevant quantum computer becomes operational can leave too little time to migrate.

Long-lived sensitive information

Government · Finance · Healthcare · Defense
Critical-infrastructure communications

THE COST OF WAITING

10–20 years

Historical standardization-to-integration horizon cited by NIST. Not a forecast for a specific deployment.

Long-lived data
Confidentiality may outlast current cryptography.

Act now
Identify vulnerable cryptography and plan migration.

An architectural gap, not only an algorithm upgrade

Encryption alone

Quantum-resistant mechanisms protect traffic. They do not establish that the gateway or firewall securing the channel is authentic or in an approved state.

Channel + device trust

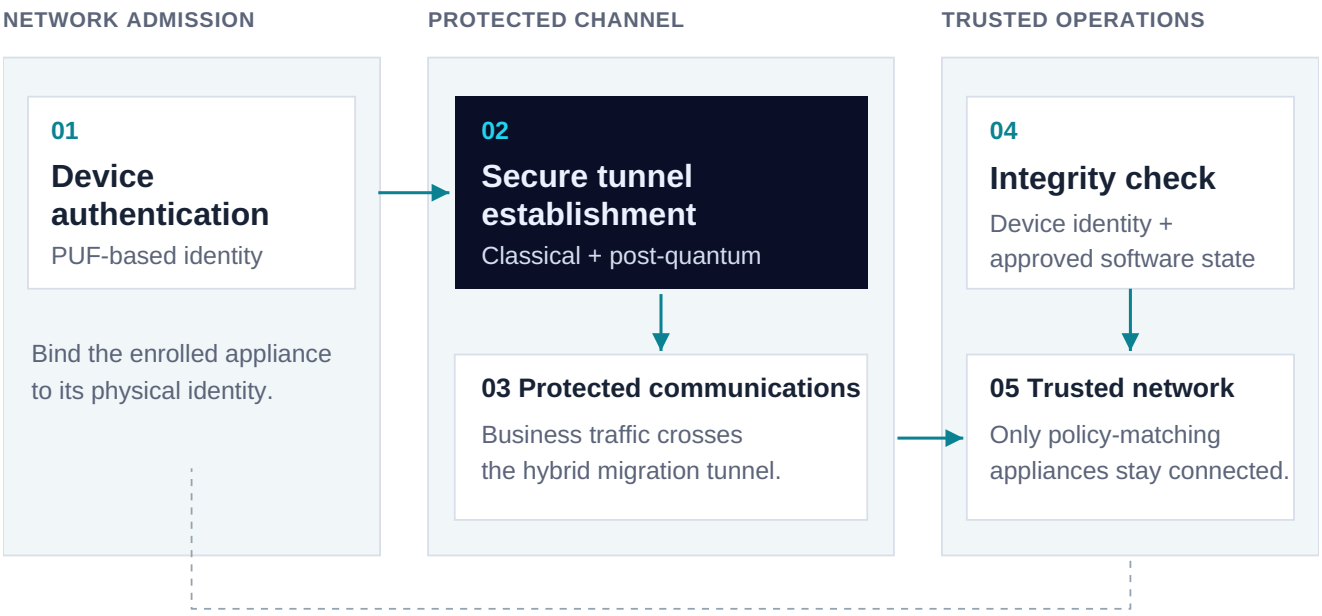
A hybrid PQC migration path addresses communications. Hardware-bound identity and integrity controls address the enrolled appliance establishing the connection.

**Protect the communication.
Trust the device. Prepare for the quantum era.**

THE AIDATACY APPROACH

Trust the channel. And the appliance.

iCyWALL brings hybrid post-quantum cryptography and PUF-based hardware identity into one architecture. Protect communications while checking the identity and approved state of the device securing them.



ONE TRUST MODEL: THE CHANNEL AND THE APPLIANCE

Validate interoperability, hardware identity and approved device state before scaling.

Conceptual workflow from the use-case source. Device authentication, hybrid tunnel establishment and integrity policy address different parts of the communication lifecycle.

What PQC contributes

Hybrid cryptography combines classical and post-quantum mechanisms during migration. The architecture supports a staged rollout that preserves interoperability.

What PUF contributes

A Physical Unclonable Function produces a response linked to a device's physical characteristics. It supports an identity designed to be difficult to reproduce and binds integrity checks to an enrolled appliance.

Communication confidentiality and device authenticity belong in the same trust architecture.

IMPLEMENTATION

From readiness to trusted operations.

Inventory the cryptography, prioritize long-lived information and validate hybrid interoperability and device trust before expanding deployment.

01 **Assessment & Scoping**

Inventory existing cryptographic algorithms, critical communication channels, confidentiality lifetimes, and trusted devices.

OUTPUT

Post-quantum readiness assessment.

02 **Architecture Design**

Define migration priorities, hybrid cryptography boundaries, PUF identity enrollment, interoperability requirements, and acceptance criteria.

OUTPUT

PQC migration architecture and roadmap.

03 **Pilot Implementation**

Deploy iCyWALL on selected critical flows with hybrid PQC communications and PUF-based device identity.

OUTPUT

Controlled post-quantum pilot environment.

04 **Performance Testing**

Measure tunnel stability, interoperability, device-authentication behavior, integrity-check coverage, and operational impact against agreed baselines.

OUTPUT

Validated pilot and test evidence.

05 **Production Rollout**

Extend approved configurations to prioritized communication flows and integrate monitoring into security operations.

OUTPUT

Production trusted-communication infrastructure.

06 **Continuous Optimization**

Track standards changes, device state, cryptographic inventory, and the next migration priorities.

OUTPUT

Governed long-term cryptographic resilience.

Deployment roadmap

PHASE 1

Discover

inventory quantum-vulnerable algorithms, critical communication channels, long-lived data, and trusted appliances.

PHASE 2

Prioritize

define migration order, hybrid-interoperability requirements, and acceptance criteria.

PHASE 3

Pilot

validate PUF-based identity, hybrid tunnels, integrity checks, and operational impact on selected flows.

PHASE 4

Scale

roll out approved patterns, integrate monitoring with security operations, and govern the remaining cryptographic backlog.

BUSINESS IMPACT

Long-term protection. Staged transformation.

Preserve long-lived confidentiality, maintain operational continuity during migration and extend trust beyond the encrypted connection to the appliance itself.

Protect

Long-Term Data Protection

Sensitive communications enter a migration path designed to preserve confidentiality against future quantum decryption risks for as long as the information remains valuable.

Migrate

Operational Continuity

Hybrid cryptography supports a staged transition, reducing the need for a single disruptive infrastructure replacement.

Verify

Trusted Infrastructure

Combining quantum-resistant communications with hardware-bound identity helps the organization evaluate both the connection and the appliance securing it.

Evidence for a production decision

Validate	What the pilot measures
Tunnel behavior	Tunnel stability and interoperability under the intended deployment conditions.
Device trust	Device-authentication behavior and integrity-check coverage.
Operational impact	Effects on operations compared with agreed baselines.
Ongoing governance	Standards changes, device state, cryptographic inventory and the next migration priorities.

The use case describes a **PQC-ready migration path**, hybrid interoperability and hardware-bound identity. These are architectural capabilities, not a universal protection percentage or a deployment-independent performance guarantee.

Protect the communication. Trust the device. Prepare for the quantum era.

NEXT STEPS

Prepare before the threat is operational.

FROM CRYPTOGRAPHIC INVENTORY TO A MIGRATION PLAN

Assess Your Post-Quantum Readiness

Start with the channels and information whose confidentiality must endure longest. Define the migration boundary and the evidence needed for a production decision.

- → Inventory vulnerable cryptography, critical communication channels and trusted devices.
- → Define confidentiality lifetimes, hybrid boundaries and acceptance criteria.
- → Pilot PUF identity, hybrid tunnels and approved-state checks on selected flows.

contact@aidatacy.com

aidatacy.com ↗

References & sources

01 NIST — Post-Quantum Cryptography
https://www.nist.gov/pqc

02 NIST — IR 8547, Initial Public Draft
https://csrc.nist.gov/pubs/ir/8547/ipd

03 NIST — SP 1800-34, Final
https://csrc.nist.gov/pubs/sp/1800/34/final

04 ETSI — TR 103 644, V1.1.1
https://www.etsi.org/deliver/etsi_tr/103600_103699/103644/01.01.01_60/tr_103644v010101p.pdf

Source basis: “USECASE iCYWALL.xlsx”, UC 01 EN narrative and source URLs. Reference descriptors identify the institution or publication. No protection percentage or latency benchmark is added.