Preparing Data Protection for the Post-Quantum Era

A Technical Overview of Adoption, Governance, and Integration

THOTQUANTUM

Table of Contents

Executive Summary

ThotQuantum is a sovereign **Data Encryption-as-a-Service (EaaS)** platform designed to protect sensitive data against today's cyber threats and the imminent impact of quantum computing on cryptography.

International standardization bodies and security agencies have established a clear timeline for the post-quantum transition. By **2027**, organizations are expected to begin migrating cryptographic systems to post-quantum-safe mechanisms, and by **2030**, the use of legacy public-key cryptography is expected to be progressively phased out for the protection of long-lived sensitive data.

This transition presents a significant challenge. Encryption is deeply embedded across applications, infrastructures, protocols, and compliance frameworks. Replacing cryptographic foundations too early introduces operational and compatibility risks, while delaying action exposes organizations to **Harvest Now, Decrypt Later** threats, where encrypted data collected today may be decrypted in the future.

ThotQuantum addresses this challenge by externalizing cryptographic complexity into a managed, sovereign platform. It enables organizations to **progressively adopt post-quantum protections** without disrupting existing systems, while maintaining continuity, auditability, and regulatory alignment throughout the transition period.

By absorbing cryptographic risk during the hybrid transition phase and supporting long-term cryptographic agility, ThotQuantum provides organizations with a controlled and defensible path from current security models toward post-quantum readiness, aligned with the 2027/2030 transition horizon.

Why Encryption Must Evolve

Modern encryption was designed under the assumption that certain mathematical problems are computationally infeasible. This assumption is now challenged by the emergence of large-scale quantum computing.

Even before practical quantum computers become available, sensitive data encrypted today may be collected and stored for future decryption, a threat commonly referred to as **Harvest Now, Decrypt Later**. This risk is particularly relevant for data with long confidentiality lifetimes, such as legal documents, health records, intellectual property, and regulated business data.

At the same time, organizations cannot simply replace existing cryptographic systems overnight. Encryption is deeply embedded in applications, protocols, infrastructure, and compliance frameworks. Abrupt cryptographic migrations introduce operational risk, compatibility issues, and regulatory uncertainty.

As a result, encryption must evolve toward **cryptographic agility**: the ability to adapt protection mechanisms over time, without compromising continuity or control.

ThotQuantum Positioning

ThotQuantum is positioned as an **external encryption layer** that decouples data protection from application logic and infrastructure constraints.

Rather than forcing organizations to redesign their systems or directly manage post-quantum cryptography, ThotQuantum provides a centralized, policy-driven encryption service that integrates with existing environments. It acts as a stable security boundary between applications and storage, while remaining adaptable to evolving cryptographic standards.

Key positioning elements include:

- **Sovereign by design**: data protection is operated under European control and governance.
- **Technology-agnostic**: ThotQuantum does not assume a single infrastructure, cloud provider, or application model.
- **Future-ready**: cryptographic mechanisms can evolve without requiring changes to client applications.

ThotQuantum's role is not to replace existing security components, but to **absorb cryptographic complexity and risk**, allowing organizations to focus on their core business.

Adoption Principles

ThotQuantum is designed around a controlled and pragmatic adoption model that reflects real-world operational constraints. Three principles guide this approach:

1. Progressive Adoption

Organizations can adopt ThotQuantum incrementally, starting with selected applications or datasets and expanding over time. This avoids disruptive "big-bang" migrations and reduces operational risk.

2. Hybrid Cryptographic Continuity

During the transition phase, classical and post-quantum cryptographic protections coexist. This hybrid approach ensures compatibility with existing systems while mitigating long-term quantum risks. The complexity of this coexistence is managed by ThotQuantum, not by client applications.

3. Security, Sovereignty, and Governance by Design

From the outset, data isolation, auditability, and compliance are integral to the platform. Governance mechanisms apply continuously throughout the lifecycle, ensuring alignment with regulatory and security requirements as cryptographic standards evolve.

The following schema illustrates how these principles translate into a **progressive adoption journey**, where cryptographic risk is transferred to ThotQuantum during the transition toward post-quantum readiness.

From Principles to Adoption States

The adoption principles described above are reflected in the progressive adoption states illustrated in the schema below. Progressive adoption enables a controlled transition from the **current cryptographic state**, through a **hybrid protection phase managed by ThotQuantum**, to a **post-quantum ready state**. Hybrid cryptographic continuity ensures protection and compatibility during the transition, while security, sovereignty, and governance apply consistently across all phases of the journey.

PROGRESSIVE

ADOPTION TO POST-QUANTUM SECURITY

Cryptographic Risk

Managed by ThotQuantum

CURRENT CRYPTOGRAPHIC STATE

Existing applications, data, and hybrid cloud environments relying on classical cryptography.

HYBRID PROTECTION WITH THOTQUANTUM

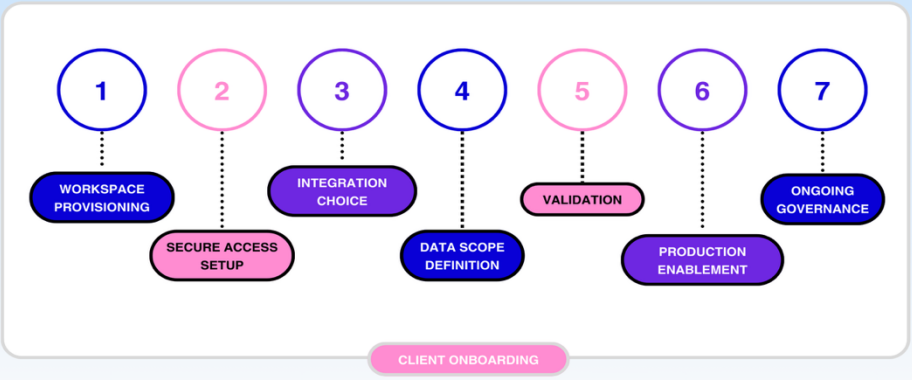
ThotQuantum introduces a hybrid encryption layer that absorbs cryptographic risk, enables progressive adoption, and ensures continuity with existing systems.

POST-QUANTUM READY STATE

Primary reliance on post-quantum cryptography, supported by cryptographic agility, long-term confidentiality, and regulatory alignment.

GOVERNANCE & CONTINUITY (ACROSS ALL PHASES)

Ongoing compliance, auditability, and adaptation to evolving cryptographic standards.



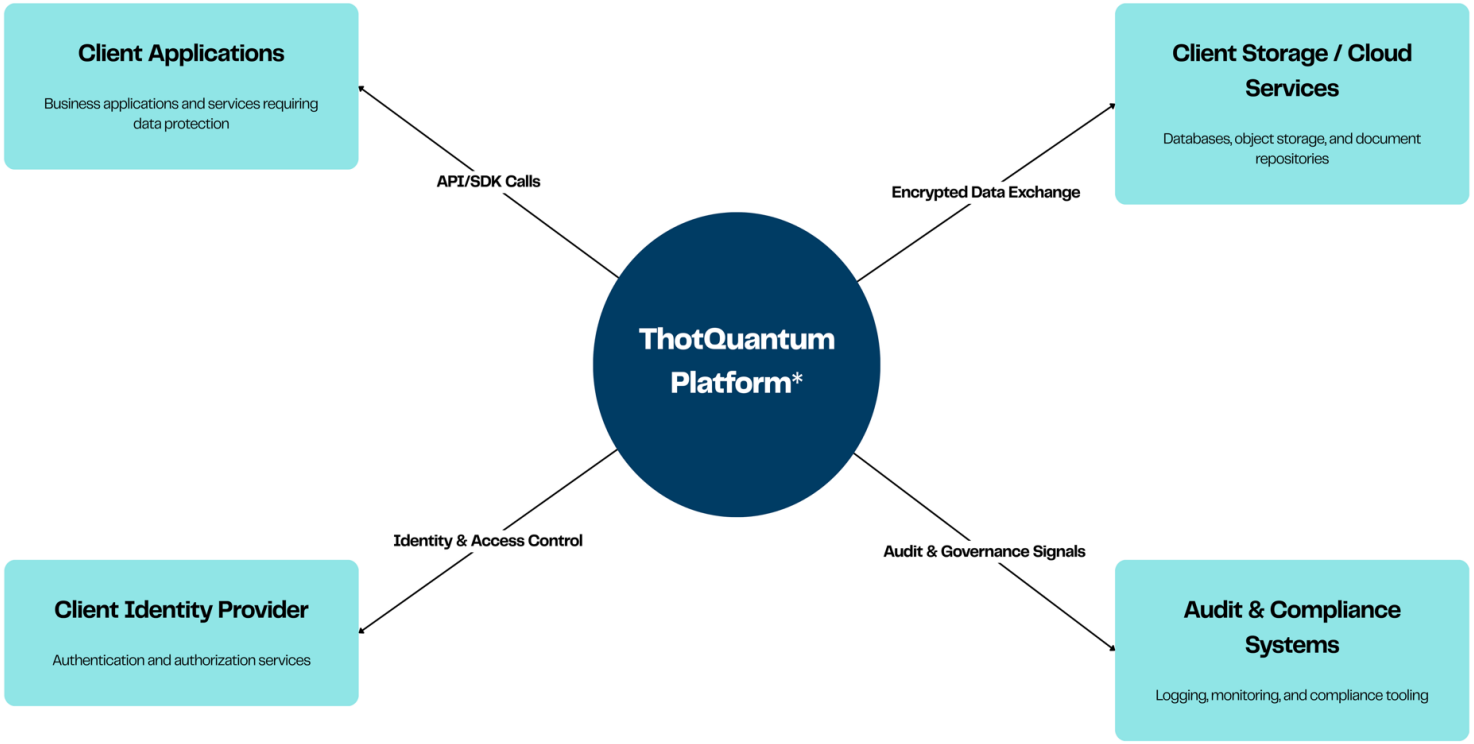
High-Level Architecture Overview

ThotQuantum integrates as an external encryption service within existing client environments. Applications interact with the platform through authenticated API or SDK calls, while encrypted data remains stored within client-managed databases, cloud services, or document repositories.

The platform does not store client business data and does not require direct access to storage systems. Instead, it provides a centralized, policy-driven encryption boundary that decouples cryptographic protection from application logic and infrastructure constraints.

Identity, access control, auditability, and governance are integrated by design, allowing organizations to maintain full control and regulatory alignment throughout the cryptographic transition.

ThotQuantum Platform — Integration Context



*Client data remains fully under client control and is never stored within the ThotQuantum platform.

Cryptographic Approach

Design Objectives

ThotQuantum's cryptographic architecture is designed to meet the following long-term objectives:

- **Security longevity**: maintain confidentiality, integrity, and authenticity guarantees over extended time horizons, including environments subject to evolving computational capabilities.
- **Cryptographic agility**: enable controlled introduction, coexistence, and retirement of cryptographic mechanisms without architectural disruption.
    - AES
    - ECIES
    - ML-KEM
    - ML-DSA
- **Operational stability**: support migration without service interruption or forced synchronization across dependent systems.
- **Auditability and governance**: provide a clear separation between cryptographic policy, architectural intent, and technical realization.

These objectives reflect standard expectations found in regulatory, financial, and critical-infrastructure contexts.

Threat Model Alignment

The cryptographic strategy is aligned with **forward-looking threat models**, including:

- Advances in classical cryptanalysis
- Increases in computational capacity
- Emergence of new cryptographic attack classes
- Long-term data exposure risks (e.g., data harvested today and decrypted later)

Rather than attempting to predict specific future attacks, ThotQuantum adopts a **risk-mitigation approach** that assumes cryptographic primitives may become obsolete over time and must therefore be replaceable.

Architectural Principles

ThotQuantum applies several foundational architectural principles:

Separation of concerns
Cryptographic functions are architecturally isolated from application logic and business workflows. This limits the blast radius of cryptographic changes and simplifies validation and review processes.

Algorithm and mechanism abstraction
Cryptographic primitives are treated as interchangeable components within a stable framework. This abstraction layer enables evolution of cryptographic choices without altering external interfaces or system behaviour.

Defence in depth
Security does not rely on a single cryptographic assumption. Where appropriate, multiple complementary protections are used to reduce systemic dependency on any one primitive or hardness assumption.

Migration and Coexistence Strategy

A core element of the approach is **planned cryptographic migration**. ThotQuantum is designed to support:

- Parallel use of multiple cryptographic mechanisms
- Gradual transition paths rather than abrupt replacement
- Backward compatibility during defined transition windows

This coexistence model is intended to meet regulatory expectations around **change management**, **risk reduction**, and **business continuity**, and avoids "all-at-once" migrations that could introduce operational or security failures.

Standards Awareness and Compliance Orientation

ThotQuantum's cryptographic strategy is informed by:

- International and regional cryptographic standards
- Recommendations from recognized standardization bodies
- Industry best practices for regulated environments

The architecture is designed to accommodate alignment with evolving standards without requiring structural redesign, enabling compliance updates to be handled as policy-level changes rather than system-wide rewrites.

Transparency Boundaries

For security and risk-management reasons, this documentation intentionally limits technical disclosure. The following are **explicitly out of scope** for this section:

- Cryptographic parameters or key sizes
- Internal key management processes
- Algorithm instantiations or protocol flows
- Implementation-specific optimizations

These details are managed through controlled technical documentation and review processes appropriate for secure environments.

From a regulatory, audit, or customer assurance perspective, ThotQuantum's cryptographic approach can be summarized as:

- **Architecture-first, algorithm-agnostic**
- **Designed for long-term evolution**
- **Aligned with modern threat models**
- **Compatible with regulated change-management practices**
- **Transparent in intent, conservative in disclosure**

The cryptographic posture of ThotQuantum is therefore defined not by fixed technical choices, but by a governance-driven approach that supports security durability, auditability, and controlled adaptation over time.

Client Onboarding Process

ThotQuantum is designed to be integrated progressively, allowing organizations to adopt post-quantum-ready encryption without disrupting existing systems. The onboarding process reflects this philosophy by focusing on controlled activation, security assurance, and long-term governance.

1. Workspace provisioning

Each client is provisioned with a **dedicated and isolated workspace** within the ThotQuantum platform.
This workspace defines the logical security boundary for cryptographic operations, policies, and audit data.

Workspace isolation ensures that encryption activities, metadata, and governance controls remain strictly separated between organizations, supporting regulatory and sovereignty requirements from the outset.

2. Secure access setup

Access to ThotQuantum services is configured using strong, identity-based authentication mechanisms.
Applications and services interact with ThotQuantum through authenticated, authorized channels, aligned with zero-trust principles.

This step establishes:

- Controlled machine-to-machine access
- Scoped permissions tied to the client workspace
- Secure token-based interaction without embedded long-term secrets

3. Integration choice

Clients select the integration approach best suited to their technical environment and operational constraints.

Supported integration patterns include:

- Direct API integration
- SDK-based integration
- Gateway encryption

This flexibility allows organizations to start with limited use cases and expand coverage over time without architectural lock-in.

4. Data scope definition

Clients define which data requires protection and how encryption is applied within their systems.

This includes:

- Identifying sensitive datasets or document types
- Determining when encryption occurs in the data lifecycle
- Aligning encryption policies with regulatory and business requirements

ThotQuantum supports consistent protection across structured and unstructured data, regardless of storage or transport mechanisms.

5. Validation

Before enabling encryption in production environments, clients perform a controlled validation phase.

This phase confirms:

- Correct encryption and decryption behavior
- Proper access control enforcement
- Availability of audit and traceability information
- Alignment with defined data protection policies

Validation ensures confidence in the integration prior to full production rollout.

6. Production enablement

Once validated, encryption workflows are activated in production environments.

ThotQuantum enables a progressive rollout, allowing organizations to:

- Gradually extend protection to additional applications or datasets
- Maintain compatibility with existing systems
- Transition toward post-quantum readiness without service interruption

7. Ongoing governance

After deployment, ThotQuantum supports continuous governance and oversight.

This includes:

- Auditability of cryptographic operations
- Policy enforcement over time
- Alignment with evolving regulatory requirements
- Support for cryptographic agility as standards and threats evolve

Governance is not a one-time activity, but a continuous process applied throughout the lifecycle of data protection.