KLARVANT

klarvant.com

QUANTUM SECURITY WHITEPAPER

Post-quantum cryptography readiness

Why your organisation must act now. A practical guide to securing your organisation against quantum computing threats before it is too late, navigating the five-pillar journey with a proven methodology.

DISCOVER IDENTIFY ANALYSE GOVERN COMPLY

KLARVANT™

— DIGITAL GOVERNANCE INTELLIGENCE —

The quantum threat is real and immediate

Quantum computing will fundamentally break the cryptographic systems that underpin digital trust, from SSL/TLS certificates to authentication frameworks. Organisations face a strategic choice: begin a methodical migration today, or face a compliance and security crisis within five years. This whitepaper outlines the proven methodology for transforming quantum readiness from an abstract concern into operational reality.

INDUSTRY VIEW

'The transition to post-quantum cryptography will demand more effort than Y2K. Organisations that have not yet planned or budgeted for this shift face an urgent priority.'

GARTNER · SEPTEMBER 2024

Two critical dates: R-Day and Q-Day

Q-Day

When quantum computers break RSA/ECC encryption. The timeline is uncertain, estimated across the 2030s to 2040s.

R-Day

When regulators mandate quantum readiness, expected between 2030 and 2035 for critical systems.

R-Day will arrive before Q-Day. Financial institutions cannot wait for regulatory deadlines. You need to be demonstrably ready when regulators start asking questions. The journey must begin now, not when enforcement begins.

Harvest now, decrypt later

Nation-state adversaries are actively capturing encrypted data today, intending to decrypt it once quantum computers become available. The NSA and the UK NCSC have issued explicit warnings that this threat is current and ongoing. If your organisation transmits sensitive data with a confidentiality requirement beyond 2030, you are already at risk.

CONFIDENTIALITY HORIZON

2030

CRITICAL UNDERSTANDING

Quantum threatens identity, not data encryption.

Quantum computers do not endanger all cryptography equally.

REMAINS QUANTUM-SAFE

Symmetric encryption such as AES-256 is not materially weakened and remains quantum-safe.

VULNERABLE

Public-key identity mechanisms (RSA, ECC, and digital signatures) are vulnerable to quantum attack.

THE REAL EXPOSURE

The threat is to authentication and trust, not to bulk data protection.

WHY IT MATTERS

Once identity is compromised, trust in digital systems collapses. This is why your migration must prioritise PKI, certificates, and authentication frameworks over data-at-rest encryption.

Klarvant's five-pillar methodology

A proven framework built on Klarvant's five pillars, used by organisations to move from zero quantum readiness to full PQC compliance. This methodology aligns directly with NIST and OMB guidance.

1 Discover

External cryptographic surface mapped from day 1

Most organisations lack visibility into where RSA/ECC cryptography is deployed across their public-facing infrastructure. Automated discovery using public-internet data, such as Certificate Transparency logs and DNS records, builds a comprehensive external cryptographic inventory from day 1, not after the eight or more weeks a manual survey takes.

KEY OUTPUTS

A complete map of public-facing SSL/TLS certificates; supported TLS versions and cipher suites; hosting infrastructure across your external footprint; the share of endpoints on TLS 1.3 versus TLS 1.2 or lower; the number of quantum-vulnerable certificates (RSA-2048, ECC P-256); and shadow IT and unknown external assets.

2 Identify gaps

Prioritise by business risk. Migrating everything at once is impossible and unnecessary. Multi-dimensional risk scoring based on exposure, data sensitivity, business criticality, and TLS readiness creates a phased migration plan.

3 Analyse root causes

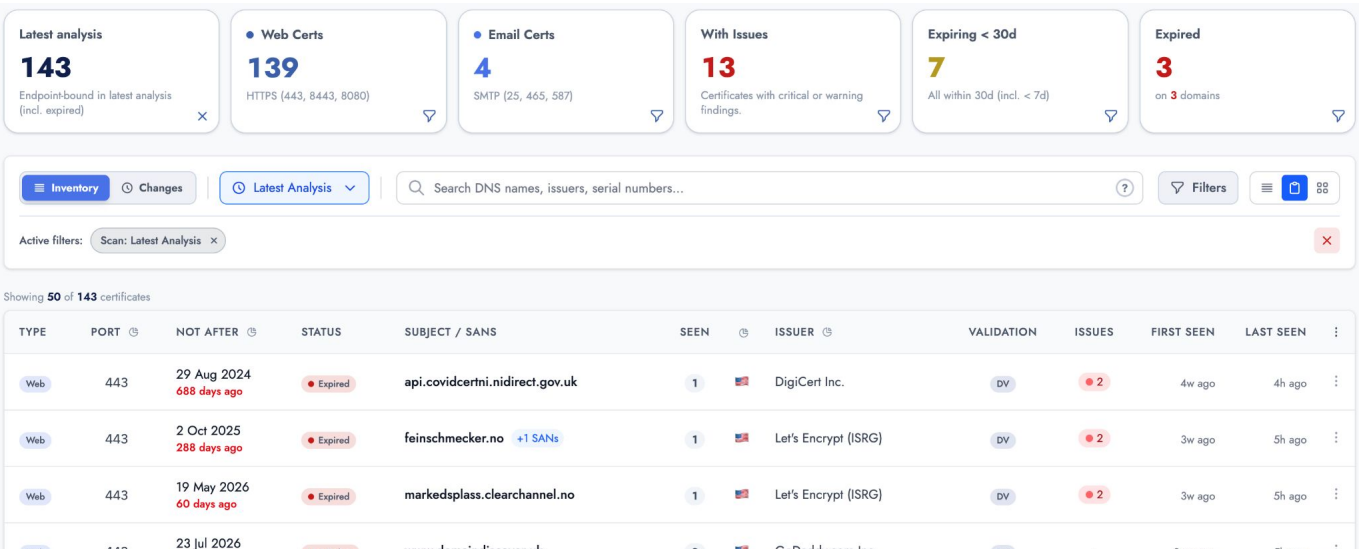
Understand the reasons behind the gaps. Is it legacy infrastructure, vendor delays, or budget constraints? Root-cause analysis drives effective remediation rather than band-aid fixes.

4 Establish governance

Create repeatable processes. Implement continuous monitoring, define ownership, establish escalation paths, and integrate PQC readiness into existing change-management and risk frameworks.

5 Ensure compliance

Meet regulatory requirements. Track progress against NIST timelines, generate audit reports, and maintain documentation for regulatory reviews and board reporting.



Three compelling reasons to act now

1 Active threat: harvest now, decrypt later

The harvest-now, decrypt-later attack is not theoretical. Sophisticated adversaries are capturing encrypted traffic today, knowing they can decrypt it within five to ten years as quantum computers mature.

SECTOR	AT-RISK DATA	CONFIDENTIALITY
Government	Classified communications, strategic planning	20+ years
Healthcare	Patient records, genomic data	Lifetime
Financial services	Transaction records, customer PII	7–10 years
Critical infrastructure	SCADA communications, OT networks	10–30 years
Intellectual property	Proprietary designs, R&D data	5–15 years

2 Compliance and regulatory pressure

Federal mandates are already in place and industry regulations will follow. Laggards face failed audits and penalties, loss of federal contracts and certifications, higher insurance premiums or denied cover, and customer attrition driven by security concerns.

3 The migration takes years

PQC migration is not a simple software patch. It is a multi-year transformation affecting TLS libraries, PKI, applications, cloud dependencies, and legacy systems.

CRITICAL TIMELINE

If your data must stay confidential beyond the time it takes to migrate plus the estimated arrival of quantum computers, you are already in the harvest-now, decrypt-later risk window.

Your path to quantum readiness

This timeline aligns with NIST IR 8547 and OMB M-23-02 guidance. Adjust it to your organisation's risk profile and resources.

1

Phase 1 · Next 90 days: discovery and assessment

Weeks 1 to 2: launch automated cryptographic discovery across all domains and brands. Weeks 3 to 4: review findings and identify Tier 1 critical assets. Months 2 to 3: conduct root-cause analysis, engage vendors for PQC roadmaps, and draft a migration policy. The leadership deliverable is a quantum-readiness assessment showing the share of assets that are quantum-vulnerable, a prioritised migration plan, and budget and resource requirements.

2

Phase 2 · Months 3 to 12: tactical execution

Migrate all Tier 1 endpoints to TLS 1.3 for crypto-agility, fix certificate hygiene (expiring certificates and weak algorithms), begin Tier 2 migration, and initiate hybrid PQC testing with key vendors. Note that standard TLS 1.3 alone does not protect against harvest-now, decrypt-later attacks; hybrid PQC key exchange is required for quantum-safe protection.

3

Phase 3 · Years 2 to 3: hybrid PQC deployment

Deploy hybrid (composite) certificates using a dual-signature approach that combines NIST-approved PQC algorithms with RSA/ECC, test compatibility across your ecosystem, and establish PQC certificate lifecycle management.

4

Phase 4 · Years 4 to 5: full PQC migration

Complete the migration to quantum-safe algorithms, decommission quantum-vulnerable systems, and achieve full compliance with federal timelines.

5

Phase 5 · Ongoing: cryptographic agility and monitoring

Build a modular, pluggable cryptographic architecture for rapid algorithm changes. Assume algorithms can fail and design for agility, not just PQC compliance. PQC is one migration, not the final migration; the win is being able to change algorithms without a complete rewrite.

Build support across your organisation

STAKEHOLDER	KEY MESSAGE
Executive leadership	The HNDL threat is active now. Gartner says this is bigger than Y2K. Federal timelines require action by 2030 and 2035.
Board / audit committee	A fiduciary duty to protect long-term sensitive data. OMB M-23-02 sets the expectation for migration plans and annual reporting.
CFO / budget	The cost of inaction is a $4.88M average breach, plus regulatory fines and reputational damage. Starting now spreads cost over five to ten years rather than crisis spending in two to three.
Infrastructure teams	TLS 1.3 migration is the first step. Automated discovery provides visibility you have never had. A dual-track approach fixes urgent issues while modernising for the future.
Procurement / vendors	All suppliers must provide PQC roadmaps. Include quantum-safe requirements in RFPs and migrate away from vendors without credible plans.
CHRO / talent	Start building quantum cryptography expertise now through graduate programmes and internal training. Waiting means competing for scarce talent at premium prices in three to five years.

CRITICAL SUCCESS FACTOR: CERTIFICATE AUTOMATION

PQC migration cannot succeed with manual certificate management. Organisations must ensure platforms support larger PQC certificates (4 to 8KB versus 1 to 2KB for RSA), plan for automated hybrid certificate deployment, and implement ACME protocol support for certificate lifecycle management at scale. Your discovery phase provides the foundation: you cannot automate certificate management for assets you do not know exist.

Three actions you can take now

01

Run a readiness assessment

Get complete visibility into your TLS versions, cipher suites, and certificate posture. Identify the Tier 1 critical assets that need immediate attention, and establish baseline metrics that let you measure progress and demonstrate posture to regulators, customers, and partners.

02

Brief leadership on the timeline

Share the Gartner warning, the NIST 2030 and 2035 guidance, and the HNDL threat. Position this as a multi-year strategic initiative that requires budget and resources now.

03

Engage your top five vendors

Ask for documented PQC migration roadmaps and certificate automation capabilities. Confirm their timeline for TLS 1.3 and hybrid PQC, and how their platform handles automated certificate lifecycle management at PQC scale.

What success looks like

Organisations that begin their PQC journey today will:

- Achieve a complete cryptographic inventory from day 1, not after weeks.
- Meet regulatory timelines, on track for NIST 2030 and 2035 guidance.
- Demonstrate leadership, using quantum readiness as a differentiator.
- Prioritise effort based on risk, focusing where it matters most.
- Avoid crisis mode, with methodical migration over five to ten years.
- Protect long-term data by reducing the HNDL risk window.

THE BOTTOM LINE

The question is not whether to migrate to post-quantum cryptography. It is whether you will do it strategically, or in crisis mode. The quantum threat timeline is uncertain, but the need to act is not.

References

Gartner, 'Post-Quantum Cryptography', Mark Horvath, September 30, 2024.

NIST, 'NIST Releases First 3 Finalized Post-Quantum Encryption Standards', August 13, 2024.

NIST FIPS 203, 'Module-Lattice-Based Key-Encapsulation Mechanism Standard', August 2024.

NIST FIPS 204, 'Module-Lattice-Based Digital Signature Standard', August 2024.

NIST FIPS 205, 'Stateless Hash-Based Digital Signature Standard', August 2024.

NIST IR 8547 (Draft), 'Transition to Post-Quantum Cryptography Standards', November 2024.

IBM Security, 'Cost of a Data Breach Report 2024', July 2024.

General Dynamics IT, 'Quantum Waves', October 2024.

The White House, 'National Security Memorandum (NSM-10)', May 4, 2022.

Office of Management and Budget, 'Memorandum M-23-02', November 18, 2022.

NSA, 'Quantum-Readiness: Migrating to a Quantum-Resistant PKI', August 2023.

NSA, 'Quantum Computing and Post-Quantum Cryptography', August 2021.

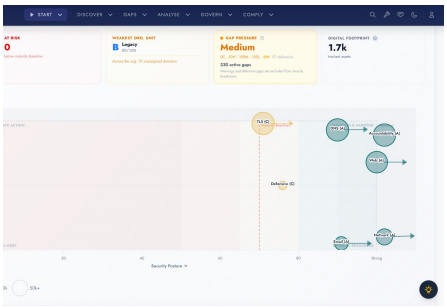
UK NCSC, 'Preparing for Quantum-Safe Cryptography', November 2020.

Global Risk Institute, 'Quantum Threat Timeline Report 2024', January 2024.

Capgemini Research Institute, 'TechnoVision 2024', 2024.

About Klarvant

Klarvant's Namespace Command provides zero-integration digital governance, with 13 specialist AI analysis areas and a personal advisor. The platform continuously discovers and analyses your external digital infrastructure, and governs it through verified ownership and the five-pillar lifecycle: Discover, Identify, Analyse, Govern, Comply. It maps over 7 billion unique identifiers globally and helps organisations understand, govern, and secure their complete digital footprint, from domains and subdomains to URLs and certificates.



Your certificate, TLS endpoint, protocol and cipher posture is served on demand over MCP and the open A2A standard, so your teams, and their AI agents, can plan, prioritise and evidence the transition. Agent-ready by design.

7Bn+

unique identifiers mapped globally across primary domains and subdomains.

Begin your quantum-readiness journey

Contact us to schedule a quantum-readiness assessment and see how Klarvant can help your organisation navigate the transition to post-quantum cryptography.

GET YOUR ASSESSMENT

sales@klarvant.com