# Delivering Cryptographic Posture Management at Scale

An integrated approach to modernize your cryptographic posture and build post-quantum resilience

IBM®

ENTRUST
SECURING A WORLD IN MOTION

# Cryptography Has Become an Invisible Operational Risk


of organizations say that managing their cryptographic assets is extremely or very difficult[1]


of organizations reported "a lack of clear ownership" as a top challenge for enabling PKI applications and post-quantum transition[2]


of U.S. cybersecurity practitioners believe quantum computing can break RSA/ECC in five years[3]

Cryptography underpins almost every digital business process, yet across most large enterprises it remains fragmented, poorly governed, and largely invisible until something breaks. Certificates expire, trust chains fail, gaps surface during audits, or services go down. These failures are not edge cases; they are a direct result of cryptographic sprawl across cloud, on-premises, and hybrid environments.

At the same time, organizations face rising external pressures. Certificate lifetimes are shortening, audit expectations are increasing, and regulators are demanding continuous evidence of control. Quantum computing compounds this risk. Long-lived data, identities, and trust chains protected today by RSA and ECC are exposed to "harvest now, decrypt later" (HNDL) threats, while most enterprises lack the crypto-agility required to migrate safely without disruption.

## These dynamics create two urgent and inseparable needs:

- **Continuous cryptographic posture management today** to prevent outages, reduce audit stress, and regain control of enterprise cryptography.
- **A governed, phased path to post-quantum readiness** that delivers migration priorities aligned to business risk rather than just technical exposure.

## A Joint IBM Consulting and Entrust Response

IBM Consulting and Entrust have partnered to address this challenge with an integrated, enterprise-wide approach. IBM Consulting brings strategy, assessment, and orchestration for complex, multi-year transformations. Entrust provides the Cryptographic Security Platform (CSP), a unified control plane for PKI, certificates, keys, secrets, and hardware-anchored trust. Together, they deliver a structured business transformation journey from fragmented cryptography to a governed, crypto-agile, and post-quantum-ready operating model.

1 https://www.entrust.com/resources/reports/ponemon-post-quantum-report-2026
2 https://www.entrust.com/company/newsroom/post-quantum-cryptography-awareness-is-high-but-widespread-action-lags-finds-2024-global-entrust-report
3 https://www.entrust.com/company/newsroom/entrust-global-report-finds-cryptographic-visibility-stagnant-as-quantum-threat-nears

## The Joint Solution

The IBM Consulting and Entrust joint solution delivers enterprise cryptographic posture management as a foundation, then based on the client requirements, evolves that capability into governed post-quantum readiness. This integrated approach aligns people, processes, and technology around a single system of record for cryptography.

The result is a structured, end-to-end, quantum-safe transformation journey, from fragmented cryptography to governed, crypto-agile, post-quantum readiness.

**IBM Consulting** provides strategy and orchestration to assess, plan, and integrate cryptographic modernization end-to-end.

**Entrust** provides the Cryptographic Security Platform to deliver continuous visibility, automation, and lifecycle management, rooted in hardware-anchored trust.

### Business and Technical Inventory

Map business services and regulatory obligations and build a bottom-up view of cryptographic configurations, certificates, keys, and data flows.

### Roadmap and Accelerators

Produce a sequenced, risk-based quantum readiness plan supported by AI accelerators that extract cryptographic metadata at scale.

### Integration and Orchestration

Design and integrate crypto-agility/ PQC patterns across applications, data, cloud, and identity: turning plans into execution.

### Unified Control Plane Visibility

Entrust CSP provides enterprise-wide (cloud/on-premises/hybrid) visibility into the cryptographic estate.

### Lifecycle and Crypto-Agility

PKI and certificate lifecycle management with capabilities that support the transition from classical → hybrid → PQC.


### Hardware Root of Trust and Operationalization

nShield HSMs and CodeSafe for hardware-anchored trust, plus deployment and configuration enablement to run it at scale.

# Two Engagements, One Structured Journey

Organizations are at very different points in their cryptographic maturity, yet most face the same reality: Fragmented cryptography creates immediate operational risk, while quantum computing introduces a long-term, high-impact challenge that cannot be ignored. To meet organizations where they are and support progress without disruption, IBM Consulting and Entrust deliver two complementary engagements:

## I) Cryptographic posture management

**Allows enterprises to regain control of fragmented certificates, keys, secrets, and cryptographic processes across hybrid environments**

**Business Value:**

By moving cryptography from manual, reactive work to automated, policy-driven operations, IBM Consulting and Entrust help reduce the cost of "cryptographic housekeeping" and the time spent chasing renewals, incidents, and audit evidence.

**Business outcomes:**

- Fewer certificate- and key-related outages through automated discovery and lifecycle management
- Reduced cryptographic sprawl with clear ownership and standardized controls
- Continuous, audit-ready evidence to support regulatory and internal compliance
- Lower operational cost and effort by replacing manual, reactive processes with policy-driven automation

## II) Post-quantum readiness

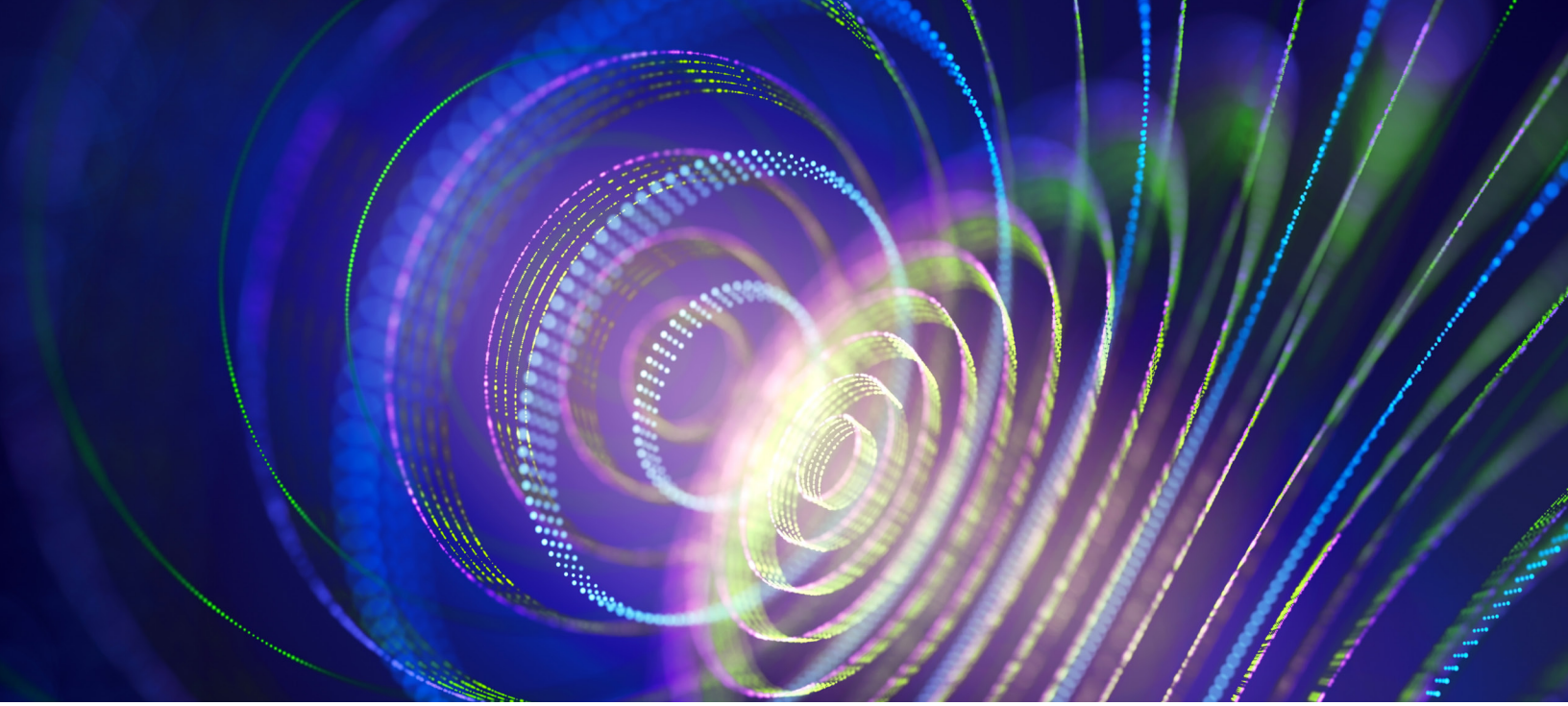
**Enable enterprises to identify, prioritize, and safely migrate quantum-vulnerable cryptography**

**Business Value**

IBM Consulting and Entrust help organizations avoid expensive last-minute quantum remediation by establishing clear visibility into cryptographic exposure, a phased migration roadmap, and an operating model for safe hybrid/PQC transitions. By consolidating controls and automating workflows in a single platform, clients reduce overhead, improve auditability, and build durable post-quantum resilience.

**Business outcomes:**

- Clear visibility into quantum-vulnerable systems, data, and trust chains
- A phased, business-aligned migration roadmap that avoids rushed Q-Day remediation
- A crypto-agile target architecture supporting classical, hybrid, and PQC cryptography
- Sustained readiness through continuous monitoring, policies, and automated workflows



## The Entrust and IBM Consulting Difference

The partnership between IBM Consulting and Entrust brings together complementary strengths, delivering unified control, quantum resilience, and stronger security across your enterprise.

- **Comprehensive enterprise-wide cryptographic control and remediation plane:** Deliver visibility, policy enforcement, and governance across the entire cryptographic estate.
- **Accelerated cryptographic maturity aligned to business risk:** Prioritized and measurable cryptographic transformation roadmap mapped to business outcomes.
- **Stronger security with lower operational complexity:** Preserve existing investments with a unified, vendor-neutral platform that eliminates fragmented tools across legacy systems, cloud services, and DevOps pipelines.
- **Post-quantum readiness as a governed operating capability:** Crypto-agile PKI, centralized key management, and FPGA-based hardware root of trust governed through an operating model that sustains compliance, adaptability, and quantum-safe security.

**Request a discovery call today to assess your cryptographic posture, understand your quantum exposure, and define a business-aligned roadmap to long-term resilience.**

## ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

## ABOUT IBM CONSULTING

IBM Consulting® is where trusted expertise meets powerful technology. As the only global consultancy within a major tech leader, we drive high-impact outcomes using advanced AI and a science-based approach to tackle your most critical challenges. Partnering directly with clients, we advise, design, build, and operate business innovation that matters and results that last.

For more information, visit IBM Quantum Safe.



entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION