HCLTech | Supercharging Progress™

HCLTech PQC: Crypto Discovery and Crypto Agility Solution

A comprehensive post-quantum data protection strategy

IBM Platinum Partner

Overview

The advent of quantum computing, while promising unprecedented advancements, poses a significant risk to traditional cryptographic systems. Emerging quantum computers have the potential to break widely used cryptographic methods like RSA and ECC, potentially rendering current data protection mechanisms obsolete. Modern organizations must prepare for the quantum age by transitioning to quantum-safe methodologies to secure sensitive data and maintain operational integrity.

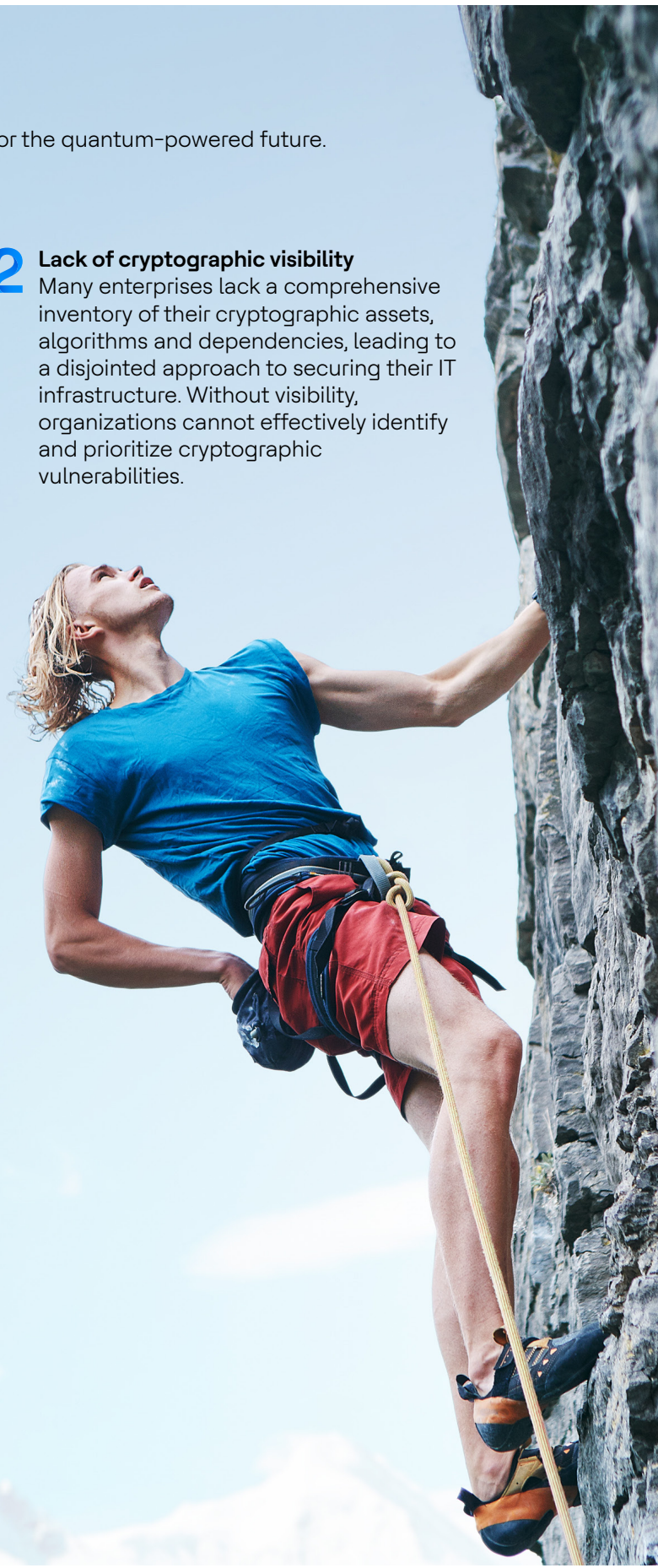
Challenges

Organizations globally face several hurdles in preparing for the quantum-powered future. These challenges include:

1 **Imminent quantum threats**
Quantum computing can break traditional cryptographic algorithms integral to securing data, transactions and communications. Once operational, quantum computers will endanger previously secure systems, making acceleration toward quantum-safe alternatives necessary.

2 **Lack of cryptographic visibility**
Many enterprises lack a comprehensive inventory of their cryptographic assets, algorithms and dependencies, leading to a disjointed approach to securing their IT infrastructure. Without visibility, organizations cannot effectively identify and prioritize cryptographic vulnerabilities.

3 **Complex infrastructure**
Organizations with hybrid infrastructures, spanning on-prem systems and SaaS applications, face unique challenges in discovering and classifying cryptographic assets. The complexity of these systems compounds the difficulty of achieving a unified cryptographic posture.



4 **Compliance pressures**
The emergence of new cryptographic standards and mandates, such as NIST's PQC standards, requires organizations to act preemptively to mitigate risks. Delayed adoption could lead to non-compliance, operational disruptions, or data breaches.

5 **Crypto agility gap**
Many systems and applications lack the flexibility to adapt to new cryptographic protocols without significant operational downtime or resource investment. This rigidity presents a major roadblock in transitioning securely to PQC.

HCLTech's PQC offering: A trusted solution for the quantum era

Crypto Discovery and **Crypto Agility** solution, powered by **IBM Guardium Crypto-Agility portfolio** is designed to address these challenges. Our solution empowers organizations to achieve quantum resilience by creating a Cryptographic Bill of Materials (CBOM), assessing cryptographic vulnerabilities and facilitating seamless adoption of **Post-Quantum Cryptography (PQC)** standards. This provides a robust cryptographic asset discovery, evaluation, remediation and migration framework. It ensures crypto agility, enabling organizations to adapt swiftly to emerging cryptographic standards, including NIST approved post-quantum algorithms. Some of the key features of our solution are as follows:

1. Crypto inventory development
HCLTech's PQC offering introduces a comprehensive scanning module enabling organizations to build a detailed cryptographic inventory, mapping out algorithms, protocols and cipher strengths across hybrid environments and on-prem systems. This scanning capability lays the foundation for creating a Cryptographic Bill of Materials (CBOM), an essential step in cataloging cryptographic assets and their dependencies.

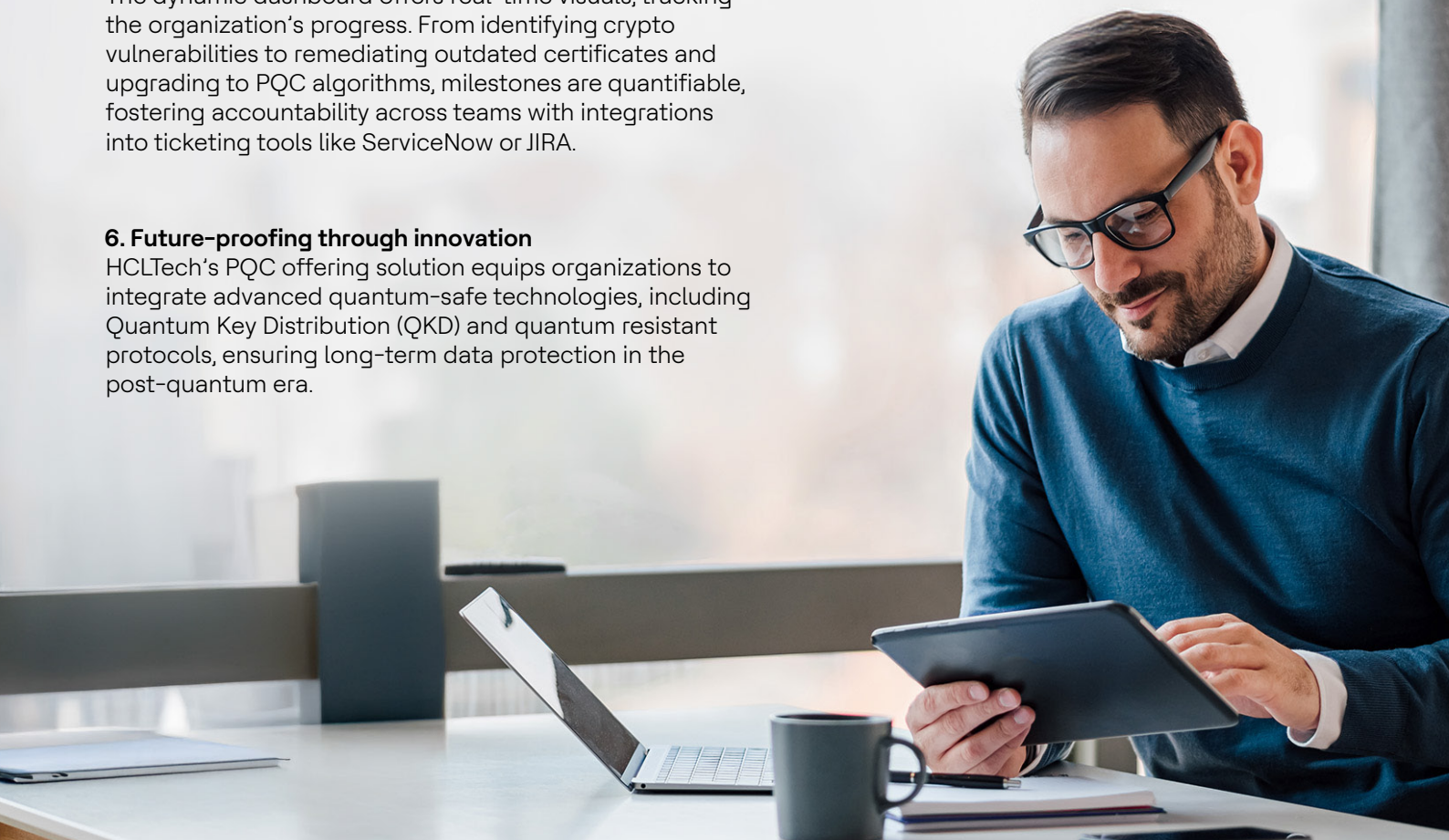
2. Cryptographic posture evaluation
Enables organizations to assess their cryptographic readiness by analyzing cryptographic frameworks, including library types, endpoints and policies. Legacy algorithms like RSA and ECC are evaluated for vulnerabilities to quantum computing attacks. Metrics and dashboards allow enterprises to visualize their current cryptographic posture and plan for remediation.

3. Ensuring policy compliance and mitigating v ulnerabilities HCLTech's PQC offering identifies weaknesses, such as outdated algorithms, improperly implemented TLS configurations and insecure cryptographic practices. It provides actionable remediation steps to align systems with emerging PQC standards. This ensures cryptographic hygiene and positions organizations for compliance with regulatory mandates.

4. Seamless transition to quantum-safe algorithms
Achieving crypto agility is at the core of the framework. Our solution prepares organizations to transition seamlessly to quantum-safe algorithms like Crystals-Kyber (ML-KEM) and Dilithium (ML-DSA), implementing quantum-resistant methods with minimal operational disruption.

5. Real-time progress tracking
The dynamic dashboard offers real-time visuals, tracking the organization's progress. From identifying crypto vulnerabilities to remediating outdated certificates and upgrading to PQC algorithms, milestones are quantifiable, fostering accountability across teams with integrations into ticketing tools like ServiceNow or JIRA.

6. Future-proofing through innovation
HCLTech's PQC offering solution equips organizations to integrate advanced quantum-safe technologies, including Quantum Key Distribution (QKD) and quantum resistant protocols, ensuring long-term data protection in the post-quantum era.

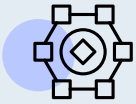


Benefits/Value delivered

HCLTech PQC offering powered by IBM, provides transformational value to organizations. It transcends mere threat mitigation and empowers them to adapt to the evolving cryptographic landscape proactively.

Cryptographic inventory for strategic planning
HCLTech's PQC offering creates a centralized, single-pane view of cryptographic assets and their dependencies. This thorough inventory enables the creation of a robust CBOM, helping organizations prioritize and strategize cryptographic upgrades efficiently.

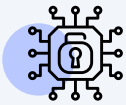
Enhanced data security with weak crypto remediation
By understanding which cryptographic components need fortification, organizations can prioritize upgrading to quantum-safe algorithms. This proactive approach mitigates risks and ensures that critical data remains secure even in a post-quantum world.



Visibility into crypto dependencies
Effective management of cryptographic dependencies, such as libraries, protocols and suites, ensures seamless integration of quantum resistant technologies. Upgraded dependencies enable organizations to handle future quantum-safe standards effortlessly.

Compliance assurance
Ensures that organizations remain aligned with emerging NIST-approved PQC standards and other compliance frameworks. This minimizes risks of non-compliance and strengthens the organization's security posture.

Crypto agility for seamless transition
By building crypto agility, systems and protocols can easily transition to quantum-safe options without disrupting ongoing operations. This capability future proofs organizational infrastructure, mitigating the costs and risks associated with rigid systems.



Holistic post-quantum protection
Enables organizations to mitigate quantum-related threats proactively. From cryptographic vulnerability discovery to implementing quantum-resistant protocols like QKD, managing lifecycle of Cryptographic objects, protect data through encryption, this solution provides a pathway to holistic, long-term quantum resilience.

Why act now?

As NIST begins rolling out final PQC standards with global adaptation deadlines, there has never been a more critical time to act. Delaying preparations can expose organizations to catastrophic consequences, including data breaches and operational disruptions. HCLTech's PQC offering is a strategic investment that ensures organizations don't just respond to risks—they lead in their defense against quantum threats.

For more information, visit the solution page on IBM

Learn more about our partnership: HCLTech and IBM Software for Security

HCLTech | Supercharging Progress™

hcltech.com