

Post-Quantum Cryptography Services



Overview

Quantum computers represent a fundamental shift in the cyber threat landscape, rendering the classical cryptography used in TLS, SSH and IPsec vulnerable. Today, adversaries are already engaged in "harvest now, decrypt later" (HNDL) attacks, intercepting and storing encrypted data with the intent to decrypt it as soon as large-scale quantum computers become available.

This imminent threat has spurred a global mandate for Post-Quantum Cryptography (PQC). As NIST finalizes PQC standards like ML-KEM and ML-DSA, cyber leaders must move beyond theoretical awareness to a practical modernization plan grounded in real-world visibility. To address this challenge, Zscaler and HCLTech have launched a joint PQC offering that combines Zscaler's quantum-ready Security Service Edge (SSE) capabilities with HCLTech's service-led crypto discovery and modernization. By leveraging real-world inline telemetry, this partnership enables organizations to identify cryptographic dependencies and transition seamlessly from PQC visibility to crypto-agile execution.



Challenges

Harvest now, decrypt later (HNDL) exposure:

Data in transit protected by classical cryptography remains at risk if intercepted now and broken later by quantum computers.

Complex transition period where hybrid will dominate: During migration, hybrid PQC key exchange (classical plus quantum-resistant) becomes essential as a safety net, however it introduces new operational requirements for validation and reporting.

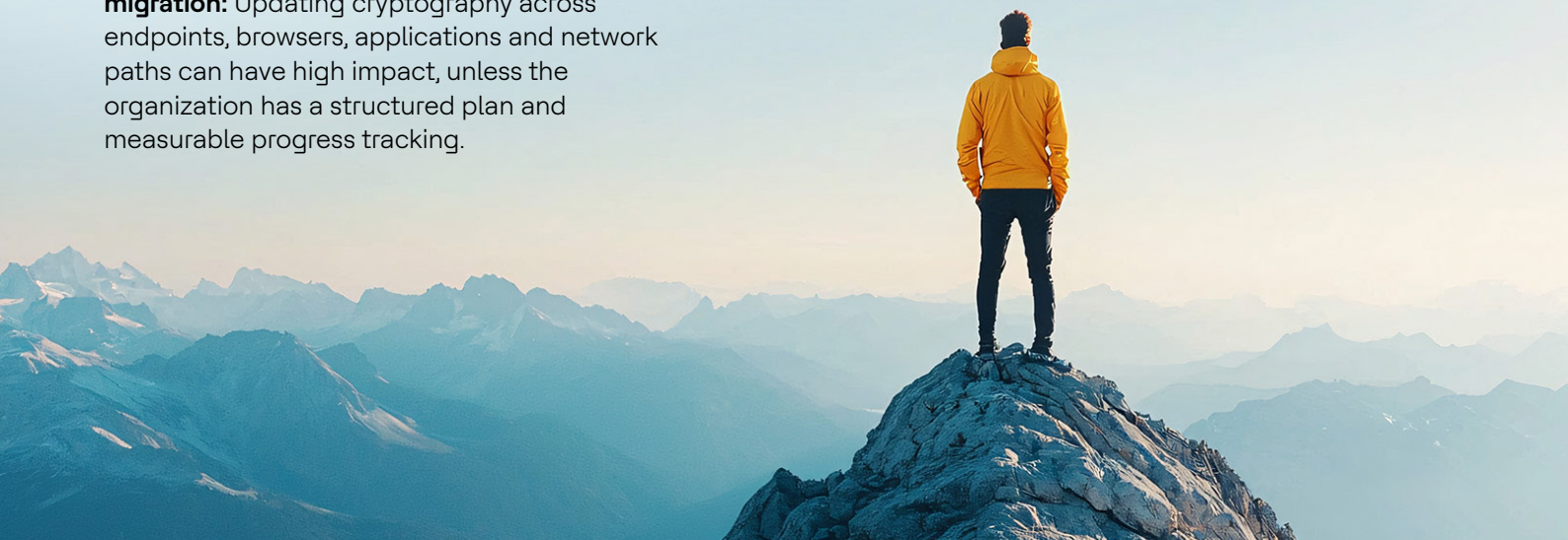
Risk of disruption or security gaps during migration: Updating cryptography across endpoints, browsers, applications and network paths can have high impact, unless the organization has a structured plan and measurable progress tracking.

Limited visibility into PQC usage in real traffic:

Many organizations cannot confidently answer which users, apps and destinations are negotiating PQC or hybrid PQC today and where they are still dependent on classical methods.

Expanding compliance and reporting needs:

Government and security agencies are mandating PQC adoption and evidence. Organizations need reporting that shows the usage of quantum ciphers across their environments.



Our solution

HCLTech and Zscaler deliver a closed-loop, security-led assessment that helps enterprises assess and advance PQC readiness by leveraging Zscaler's in-line Internet and SaaS telemetry, together with HCLTech's discovery, CryptoBOM creation, prioritization, remediation and progress-tracking services.

Quantum-ready visibility and inspection with Zscaler

Zscaler delivers first-to-market capabilities that make quantum readiness practical on a scale:

Inline SSL/TLS inspection for hybrid PQC key

exchange: Zscaler Internet Access (ZIA) supports hybrid PQC key exchange and provides real-time deep inspection of PQC traffic using NIST-standardized ML-KEM (FIPS 203). This enables decryption, inspection, policy enforcement and re-encryption for PQC sessions on a scale.

Protection even when the source server is not

PQC-capable: With Zscaler's proxy architecture, PQC can be used between the client and Zscaler independent of server capabilities, helping reduce last-mile exposure.

No policy redesign required: Threat prevention, DLP and access control policies are applied transparently to PQC sessions without changes to existing configurations.

Actionable logging for prioritization: Zscaler logs the selected TLS version and key exchange parameters, allowing teams to identify non-PQC-ready clients and prioritize upgrades.

IPsec quantum risk mitigation with PPK: Zscaler supports IPsec with post-quantum pre-shared keys (PPK), mixing an additional shared secret into IKE key derivation to keep derived keys secure even if Diffie-Hellman exchanges are later broken by a quantum computer. This provides a practical upgrade path without requiring full PQC for IPsec key exchange.



Service-led CryptoBOM and migration execution with HCLTech

HCLTech turns Zscaler-native visibility into an enterprise execution roadmap:

Crypto discovery and CryptoBOM creation:

HCLTech leverages Zscaler as a primary data source for cryptographic discovery and combines it with broader enterprise discovery to produce a CryptoBOM and dependency insights across users, applications and network paths.

PQC readiness assessment and roadmap:

Risk-based assessment aligned to emerging standards, identifying where hybrid PQC is present, where classical mechanisms remain and what to remediate first.

Remediation and crypto agility enablement:

Structured modernization planning and execution to reduce weak cryptography, strengthen crypto agility and support a safe transition to quantum-ready cryptography.

Designed for immediate value to existing Zscaler customers

Zscaler customers can gain PQC visibility and a CryptoBOM by leveraging existing Zero Trust Exchange platform functionality, without requiring additional Zscaler licenses, delivering immediate value.

Value delivered

CryptoBOM powered by real traffic data: Moves beyond theoretical inventories by incorporating Zscaler's internet and SaaS telemetry into a practical, evidence-based CryptoBOM.

Quantum-ready inspection and policy enforcement at scale: Enables decryption and inspection of hybrid PQC traffic while applying existing security controls consistently.

Reduced HNDL exposure and stronger future resilience: Hybrid PQC support and IPsec PPK capabilities help mitigate quantum risk during the transition period.

Compliance readiness with defensible reporting: Improves ability to demonstrate quantum cipher usage and progress toward PQC adoption.

Faster, lower-risk migration to crypto agility: HCLTech's services translate visibility into prioritized remediation and measurable modernization outcomes across stakeholders.

Immediate PQC visibility without new license cost: Leverages existing Zscaler functionality to provide rapid insight and savings for shared customers.

Uncover your hidden cryptographic risks today. Schedule a PQC readiness assessment to see how HCLTech can leverage your existing Zscaler telemetry to build your enterprise CryptoBOM, without the need for additional licensing.

[Click here](#) to learn more about HCLTech and Zscaler partnership.

HCLTech | Supercharging
Progress™

hcltech.com