QuSecure

QuProtect R3 for Post-Quantum Cryptography

The Integrated, Production-Ready PQC Platform for Encryption Modernization

As organizations diversify across cloud, legacy, and edge environments, hidden cryptographic sprawl and outdated encryption threaten to undermine even the best defenses. Risk exists today from 'Harvest Now, Decrypt Later' attacks and AI-driven threats that find weaknesses in encryption. Traditional security tools – focused on endpoints or firewalls – simply cannot see or fix these risks.

Organizations that focus on the encryption that secures data itself can mitigate these attacks and be better prepared for Q-Day and quantum attacks on the horizon. Unfortunately, security leaders have been told that preparing for post-quantum cryptography (PQC) would take years, cost millions, and require deep in-house expertise.

Security Modernization for Everyone

A pioneer in orchestrated cryptographic agility, QuSecure exists to address this blind spot with an approach that makes encryption modernization simple for everyone.

Our QuProtect R3 platform identifies and prioritizes quantum-vulnerable cryptography across networks, enabling leaders to create clear remediation roadmaps. Once assets are discovered, organizations can gain active mitigation and real-time reporting insights in the same platform.

Built on the value that discovery and visibility are critical to help organizations migrate, QuSecure helps clear the path to post-quantum security by providing the platform's Reconnaissance module complementary to qualified companies.

With QuProtect R3, customers get cryptographic agility with executable simplicity and clarity, without disrupting operations or incurring costly overhauls.

QuSecure

QuProtect R3 for Post-Quantum Cryptography

The Integrated, Production-Ready PQC Platform for Encryption Modernization

Three Modules, One Production Ready, Integrated Platform

QuProtect R3 provides visibility and control over cryptography itself – from discovery through to remediation.

> **QuProtect Reconnaissance Module for continuous discovery and inventory** – Gain a comprehensive, live inventory of cryptography in use for data in transit for custom assessments that easily highlight out-of-policy or vulnerable algorithms, providing actionable insights to strengthen security posture.
>
> Benefits: Eliminate months of manual crypto auditing. Easily and cost-effectively fulfill CBOM requirements. Free to qualified organizations.

> **QuProtect Resilience Module for active mitigation** – Fortify entire networks with seamless cryptographic protection for both modern and legacy systems. Low-touch integration enables crypto-agility to update encryption across all devices and systems whether PQC migration is a short-term or long-term plan. Ensure a smooth and speedy transition to PQC and zero trust without disruptions or code changes, even when algorithms are compromised or new standards emerge.
>
> Benefits: Simplify a full, cryptographic-aware migration. Pinpoint high-risk communications for immediate prioritization.

> **QuProtect Reporting Module for real-time insights** – Generate a Cryptographic Bill of Materials (CBOM) with a single click to ensure compliance with evolving standards like ensure CNSA 2.0, CNSSP 15, and GDPR, while maintaining full transparency over cryptographic inventory on the network.
>
> Benefits: Streamline compliance with on-demand visibility and control. Deliver board-ready metrics.