Cryptographic Resilience for the Quantum Era

Helping enterprises and governments protect sensitive data, strengthen cryptographic control and prepare for a quantum-safe future.

Founded in 2008 and headquartered in Canberra, Australia, **QuintessenceLabs** is a quantum cybersecurity company helping organizations strengthen data protection and build cryptographic resilience. We bring together cryptographic asset management, enterprise key management and quantum technologies to protect sensitive information today and support the transition to post-quantum cryptography (PQC).

Our capabilities span the cryptographic lifecycle—from understanding where cryptography is used to generating, managing and distributing the keys that protect enterprise data. We serve leading financial institutions, government and defence organizations, and major enterprises, including Forbes Global 2000 companies.

Why cryptographic **resilience matters**

Encryption underpins digital trust across applications, infrastructure and communications. Its effectiveness depends on the quality of cryptographic keys, how they are managed and the ability to adapt as algorithms and security requirements change. As organizations prepare for quantum computing, they need visibility into cryptographic dependencies and a practical way to prioritize and implement change while maintaining business continuity.

Our core **capabilities**

Cryptographic visibility and PQC readiness



TSF® Sentry discovers cryptographic assets and dependencies, evaluates exposure and maps findings to the applications responsible for them—helping teams turn large inventories into prioritized remediation. Integration with enterprise automation tools supports execution, while our PQC Readiness Assessment provides a risk-based migration roadmap and governance guidance.

Enterprise key and policy management



The Trusted Security Foundation® (TSF®) key & policy manager centralizes control of encryption keys and policies across on-premises, cloud and hybrid environments. Vendor-neutral integration through industry-standard interfaces helps organizations manage key lifecycles, strengthen control over sensitive data and adopt new cryptographic capabilities as requirements evolve.

Quantum random number generation



Strong encryption starts with unpredictable keys. qStream QRNG provides high-quality quantum entropy for cryptographic key generation and other security applications. Its NIST SP 800-90B certified entropy source delivers up to 1 Gbit/s of randomness, supporting demanding enterprise workloads and integration into existing security infrastructure.

Quantum-safe key distribution



qOptica provides QKD capabilities using quantum physics to protect key exchange. These technologies give organizations flexibility to design protection suited to their network requirements, security objectives and migration priorities. qConnect supports key distribution using PQC, quantum key distribution (QKD) and hybrid approaches.

Enterprise value and **practical adoption**

Our capabilities support needs ranging from protecting long-lived sensitive data and strengthening public key infrastructure to securing cloud workloads and communications. By combining visibility, risk-based planning and operational controls, organizations can focus resources on their highest-priority exposures and make measurable progress toward PQC readiness.

QuintessenceLabs works with organizations and technology partners to integrate these capabilities into broader security architectures. Standards-based interoperability and crypto-agility support a staged approach that builds on existing investments, reduces migration disruption and enables continued adaptation as threats and technologies evolve.