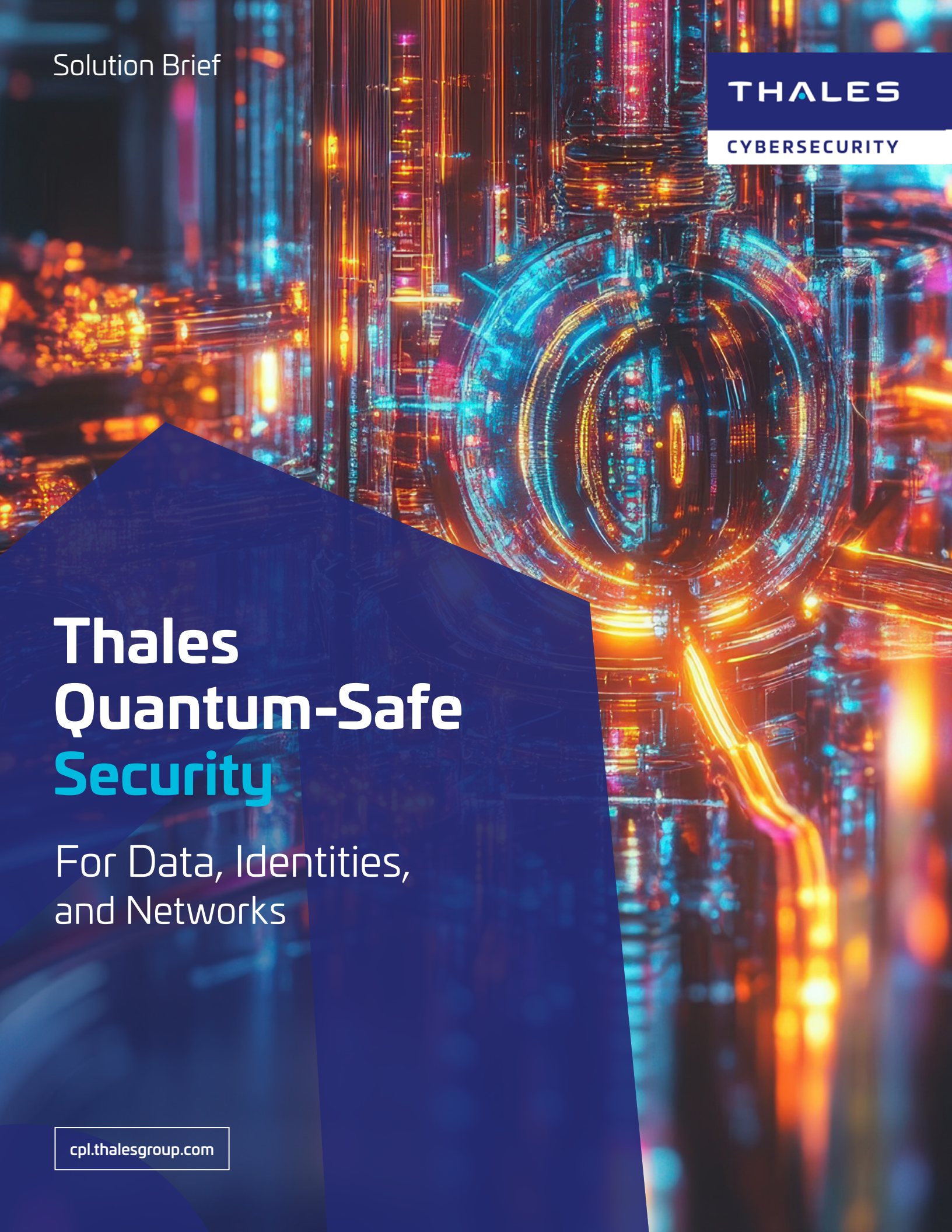
Solution Brief



THALES

CYBERSECURITY

Thales Quantum-Safe Security

For Data, Identities, and Networks

cpl.thalesgroup.com

THALES

CYBERSECURITY

Sovereign Cryptography - Crypto-Agility, HSMs & Key Management

Secure keys and cryptographic operations, identities, and critical data flows across the networks today, with a controlled migration path to PQC.

Thales provides high-assurance, crypto-agile protection for data, identities and networks across digital business, critical infrastructure and connected services. With hardware, software, on-premises, hybrid and cloud-delivered solutions, the company helps organisations discover and classify sensitive data, protect it at rest, in motion and in use, and maintain end-to-end control of keys and cryptographic processes. From key generation inside certified HSMs through encryption of data as it moves across the network, and policy enforcement across on-premises, hybrid and multi-cloud environments, Thales' products are designed for crypto-agility: algorithms, key lengths and policies can evolve without redesigning applications or networks. This underpins Thales' quantum-safe portfolio, which already delivers PQC capabilities in shipping products and provides a clear migration path from today's classical public-key cryptography to hybrid and, over time, fully post-quantum architectures.

Luna Hardware Security Modules (HSMs)

Thales Luna HSMs are FIPS 140-3 Level 3 validated, certified to Common Criteria EAL4+ and classified NATO Secret, with support for eIDAS Protection Profile EN 419 221-5. Luna HSMs provide a crypto-agile, quantum-safe hardware root of trust for a wide range of applications from the CipherTrust Data Security Platform and broader Thales solutions, to mobile and telecom workloads. Luna HSMs are among the first FIPS 140-3 Level 3 platforms to integrate NIST-standardised PQC algorithms directly in firmware, as well as extending crypto-agility to support new or sovereign algorithms. Support for ML-KEM and ML-DSA, together with quantum-safe hash-based signatures such as LMS/HSS and existing classical algorithms, enableshybrid modes so organisations can leverage PQC for key management, TLS/SSL, key exchange, PKI and code signing with minimal change to applications. PQC capabilities are available on the same Luna HSMs already in production, with the option to use external entropy sources such as quantum random number generators (QRNGs). By reusing existing integrations and tooling, organisations in long-lived, regulated environments can choose their own path to being quantum-safe – whether by starting with hybrid deployments or moving directly to full PQC solutions. Thales is working on its next-generation HSM for the quantum era. It is designed to be quantum-safe from the ground up, with a new PQC-ready crypto processor - custom-designed by Thales - to ensure high-efficiency operation, crypto agility, supply chain sovereignty while being highly scalable and multitenant with strong security isolation.

High Speed Encryptors (HSE)

Thales High Speed Encryptors (HSE) provide quantum-ready protection for data in motion across enterprise, government, defence and critical infrastructure networks. Designed to drop into a wide range of network architectures, from simple point-topoint links to meshed, hub-and-spoke and SD-WAN topologies, HSE is available as both physical and virtual platforms and delivers line-rate encryption at Network Layers 2, 3 and 4. PQC and hybrid modes have been built into certified HSE platforms for several years, so customers can introduce quantum-resistant protection without adding external components or redesigning their networks. Building on a long track record in high-assurance WAN and data-centre protection, HSE hardware uses crypto-agile, FPGAbased designs so quantum-safe capabilities can be enabled and updated via in-field firmware and policy changes. With NIST PQC algorithms implemented, HSE supports the transition from today's classical environments to PQC-ready networks, enabling hybrid classical/PQC tunnels so organisations can add quantum-safe protection while maintaining interoperability with existing devices and services. HSE appliances carry a broad set of third-party validations, including FIPS 140-3 Level 3 validation (Level 1 for virtual models), Common Criteria EAL4+ certification, and approvals for government, defence and critical-infrastructure use via NATO NIAPC and the U.S. DoDIN APL, providing proven drop-in protection for traffic across public and private networks. Transport Independent Mode (TIM) delivers out-of-band key material using NIST-specified key-derivation functions, separating key delivery from the data plane to help mitigate Harvest Now, Decrypt Later threats. Optional Quantum Key Distribution (QKD) integrations and the ability to use QRNGsourced entropy for key generation give customers additional design choices to align data-in-motion security with their preferred quantum-safe strategy.

CipherTrust Data Security Platform and Data Security Posture Management

The CipherTrust Data Security Platform provides a data-centric foundation for PQC adoption, with Data Security Posture Management (DSPM) as a core capability. DSPM in CipherTrust continuously discovers, classifies and protects sensitive data

across databases, files, applications, cloud services and SaaS environments, to reduce data security risk. The platform centralises key management, policy enforcement, tokenisation, encryption, and supports quantum-safe key establishment in TLS servers and application environments using KEM-based key exchange, while continuing to rely on Luna HSMs as the quantum-ready hardware root of trust for key generation, storage and critical cryptographic operations. This gives organisations a crypto-agile control plane to inventory cryptography, rotate keys, and re-encrypt sensitive data as PQC and hybrid algorithms are adopted.

Identity and Access Management

Thales Identity and Access Management (IAM) solutions extend quantum-ready security principles to digital identities and access control, addressing both current identity-based threats and the long-term cryptographic risks introduced by quantum computing. In modern zero-trust architectures, IAM must ensure trust not only in users, but also in the cryptographic mechanisms that underpin authentication, federation and secure access. Thales IAM roadmaps, including PQC-ready authentication devices, hybrid-cloud credentials and identity management systems, are designed to accommodate the evolution of quantum-safe FIDO, PKI and TLS profiles, ensuring that passwordless authentication can be progressively aligned with post-quantum cryptographic foundations as standards mature. This approach enables organisations to adopt phishing-resistant authentication today, while preparing for future PQC-enabled authentication devices and protocols.

PQC Enablement and Migration

Thales post-quantum readiness has evolved from isolated pilots into a broader enablement and migration programme. With PQC available in current Luna HSM firmware and well established in Thales High Speed Encryptors, and expanding to the rest of the portfolio, customers can enable quantum-safe and hybrid modes on their existing platforms in both non-production and production environments. Security and architecture teams can trial standardized algorithms such as ML-KEM, ML-DSA, LMS/HSS and hybrid profiles for PKI, TLS, code signing, key management and network encryption using existing integrations, tools, and operational processes, then roll validated configurations into deployment. Thales complements this with optional services for quantum risk and impact assessment, cryptographic posture review, and solution architecture, pilots and phased rollout, helping organisations introduce PQC in practical, low-risk steps. Together, these products, services and ecosystem partnerships mean Thales is helping customers reduce exposure now by actively enabling them to deploy quantum-safe, crypto-agile architectures today.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.