Solution Brief

THALES

CYBERSECURITY

Securing Emerging Technologies with Thales Luna HSMs

cpl.thalesgroup.com

THALES

CYBERSECURITY

A time of fundamental change

In today's digital world, enterprise and government organizations are navigating major shifts in how they operate, innovate, and protect critical systems. AI adoption is accelerating, cloud and hybrid environments are expanding, and post-quantum cryptography is moving from a future concern to a current priority. Together, these shifts are reshaping digital strategies and increasing the need for trusted, scalable, and resilient security infrastructure.

At the same time, attackers are becoming more sophisticated. Threats such as "harvest now, decrypt later" attacks highlight how adversaries are preparing for future breakthroughs while exploiting today's weaknesses. As these challenges emerge, change is becoming more prevalent across the workplace, forcing organizations to rethink how they protect data, applications, identities, and the cryptographic systems that support them.

Organizations must also respond to evolving regulations, data sovereignty requirements, distributed teams, operational complexity, and growing demands for stronger governance and control. In this environment, security is no longer just about protecting individual systems, but about maintaining trust across an increasingly connected digital ecosystem.

The risk of emerging technologies

- The increase in data and digital services is making security more complex, and leaving sensitive data at a greater risk than ever before
- IoT is expanding the attack surface with every device, and if that device is at the core, then a single attack can result in an organization being inoperativ
- Quantum computing is accelerating the need for post-quantum readiness, especially for organizations protecting sensitive data, digital identities, and critical transactions
- 5G allows incredible scale but presents the same risks as previous cellular network generations
- With emerging technologies introducing more vulnerabilities and areas for cyber-attack, the need for encryption, protection and authentication controls in today's digital journey is an obvious one

Concerns about quantum computing have matured, reflecting a deeper understanding of the risks and increased efforts toward mitigation. Future decryption of existing data, known as harvest now, decrypt later (HNDL), is identified as the top risk, cited by 61% of respondents.

Thales Data Threat Report 2026

The digital transformation continues

Organizations are modernizing their businesses, processes, and products by implementing faster, frequently changing digital technologies, including applications designed to support post-quantum readiness. They are becoming increasingly dependent on an expanding amount of data to increase customer loyalty by enhancing and personalizing the customer experience; using analytics to make faster, more accurate decisions, improving operational efficiencies and driving business; and reducing downtime and errors in order to increase revenues.

The importance of integrity, confidentiality and trust

A root of trust is the foundation of a cryptographic system. Digital security is dependent on cryptographic keys that encrypt and decrypt data and perform functions such as signing and verifying signatures. Ensuring the integrity of those keys, digital identities and the cryptographic functions within a secure environment such as an HSM is paramount to establishing confidentiality and trust between devices, identities and transactions.

Need for a strong foundation of trust

A strong foundation of trust for your digital security means you are protected without compromising agility, usability or scalability so that you can meet the high demands of industry regulations and audit requirements in addition to achieving your business and revenue goals.

Thales Luna Hardware Security Modules (HSMs) have been protecting businesses and people for decades, and evolving over the years to meet the challenges of new technologies. Organizations rely on Luna HSMs as their hardware root of trust, providing the following benefits:

- **Reduce risk.** Protect your critical digital infrastructures with a strong security architecture that is purpose built, certified, and crypto-agile. As an IT security professional, secure your data and identities with strong authentication and role separation, and a keys-in-hardware approach.
- **Ensure flexibility and visibility.** Strategic data and identity protection ensures flexibility and visibility by securing encryption keys, critical data and digital identities wherever they may be.
- **Easily install, provision and manage Luna HSMs.** Meet SLAs and reduce downtime with streamlined operations. Designed for today's lights out data centers, Luna HSMs are operationally graceful, reliable and centrally managed.
- **Simplify integration and development.** With a wide variety of APIs, flexible deployment options and superior performance, you can quickly secure hundreds of applications with our out-of-the-box technology partner integrations.

Root of trust for emerging technologies

FIPS 140-3 Level 3-validated Luna HSMs play a critical role in protecting applications using emerging technologies:

- **Post-quantum crypto agility.** Futureproof your organization with the flexibility to change protocols, keys and algorithms on the fly, quickly react to cryptographic threats, and enable quantum-safe algorithms today.
- **Internet of Things (IoT).** With the expansion of attack surfaces and an increased number of end points, you need to ensure devices and communications are properly secured. IoT relies on a strong root of trust to identity and communicate with all of the devices. Implement strong access controls, meet compliance, and ensure data integrity by creating secure digital identities for your IoT applications, physically and logically securing encryption keys with Luna HSM's strong security architecture.
- **Digital Assets.** Digital asset ecosystems rely on trusted cryptographic operations to secure wallets, custody platforms, asset tokenization services, blockchain infrastructure, and transaction signing. Protect private keys and reduce operational risk by generating, storing, and managing keys within the secure confines of a tamper-resistant Luna HSM.
- **5G /mobile.** Although 5G is ready to transform industries, it does present risks to an organization such as an increase in entry points for attackers, and a threat to data integrity, availability and confidentiality. Secure 5G data with a hardware root of trust, ensuring protection of the master storage key that encrypts all identities issued to devices; strong entropy; and strict authentication controls.
- **BYOK/HYOK/DKE.** Maintain control over your encryption keys by creating, managing and storing them securely in a hardware root of trust, following best practices to always store your keys separately from your data. Use those same keys in multiple clouds so you aren't tied to any one cloud service provider, and repatriate or move your data if need be.
- **AI.** Protect both the AI model and its input data with robust cryptographic mechanisms to ensure confidentiality, integrity, and trustworthiness of the AI system.

As AI adoption, cloud expansion, and post-quantum readiness reshape digital ecosystems, organizations need trusted encryption, authentication, and stronger protection for cryptographic keys to secure critical operations and maintain digital trust.

Top Luna HSM features that make your transformation easier

Rely on Luna HSMs as your foundation of digital trust, protecting your organization's devices, identities and transactions across your cloud, digital assets, IoT, PKI and other critical infrastructure.

Top 12 benefits to selecting Luna HSMs:

1. Ensure your critical encryption keys and digital identities are always secure and always know their whereabouts by generating, managing and storing them in a hardware root of trust by default.
2. Establish trust and integrity for your data with a strong, crypto-agile security architecture that supports evolving requirements while providing side-channel attack protection, audit logging, M of N authentication, multi-factor authentication, and extended return on investment.
3. Easily and cost-effectively meet your compliance needs from GDPR and eIDAS to PCI-DSS with the most certifications in the industry including FIPS 140-3, Common Criteria, IT, BSI, and more. Have complete trust in your infrastructure, backed by a certified HSM cryptographic foundation that is internationally recognized.
4. Secure over 400 tested, documented, 3rd party applications, extending your return on investment.
5. Control your keys when encrypting data in the cloud and using cloud service provider tools and applications by bringing your own key.
6. Quickly react to threats by implementing crypto agile, alternative means of encryption to support traditional and emerging use cases.
7. Future proof your organization by implementing quantumsafe algorithms, securing your organization's users and data today and into the future.
8. Meet the SLAs of demanding high transaction volume applications with scalable, high throughput performance.
9. Keep your organization's infrastructure operational and maximize uptime with Luna HSMs. Remove single points of failure and always keep keys secure with an architecture that stresses reliability and durability, as well as hardware-based backup for disaster recovery.
10. Easily manage and monitor your HSM resources, saving time, budget and resources. Quickly provision HSMs without the need for crypto experts; monitor their health; and receive alerts for events that require attention.
11. Deploy in modern data centers with IPV6, optional 10G fibre connectivity, and low power requirements, and reduce TCO with remote management.
12. Move freely between on-premises, cloud, hybrid and multi-cloud while ensuring your infrastructure, applications and users are secure regardless of the use case. Luna HSMs simplify hybrid environments, don't tie you to one specific location or cloud service provider, and provide you with key ownership and control with all cryptographic operations being performed in the HSM. Perform the same crypto with any of our on-premises and cloud-based HSM form factors, leveraging the same integrations, APIs and mechanisms, and the same levels of security across the board.

Selecting the right solution for your data protection needs

For more than 30 years, Thales has been the market leader continuously innovating its high-assurance FIPS 140-3 validated Luna HSMs to meet evolving security and compliance needs. Governments and the most trusted brands in the world rely on Luna HSMs as their root of trust to protect critical IT infrastructure for PKI, code signing, TLS, and database encryption, as well as emerging technologies including AI, cloud and post-quantum cryptography. This foundation of digital trust enables crypto agility, data ownership in any environment, and a hybrid or multi-cloud data protection solution.

Contact us to learn more about how Thales Luna HSMs can provide a foundation for your digital trust needs today and into the future.

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.