cpl.thalesgroup.com

THALES

Securing Emerging Technologies with Thales Luna HSMs

A time of fundamental change

In today's digital world, enterprise and government are in a state of flux. Organizations are optimizing by taking workloads to the cloud, or forging ahead transforming, taking advantage of a wide variety of emerging technologies. They are revisiting their strategies due to unforeseen circumstances such as the Covid-19 pandemic, while others are standing still unsure of what to do. And some are rejiggering existing applications to fit into new technologies, or reinventing how they build products and services in a drive to become more efficient; flexible; and competitive.

Security risks and challenges are also evolving. Hackers are becoming more sophisticated, not only focusing on traditional attacks but also engaging in simple approaches that gain access to data. Hackers are searching for holes while organizations are transitioning to a larger remote workforce with fewer resources; and workers less versed on the latest compliance mandates are trying to meet short timelines.

Change is also prevalent in the environments where we work and store our data. Some organizations are racing to the cloud, while others have decided to repatriate, and still others are leveraging multiple cloud service providers and hybrid cloud infrastructures. More temporary workers, more remote workers, rapid cloud migration and development, and a need for automation are also present - the list goes on.

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 inoperative
- Quantum computers will soon be able to break today's encryption algorithms, so critical information such as personal health records and genetic data harvested today will be exposed tomorrow
- 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

49% of companies are saying they are either agressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility.

Thales Data Threat Report 2020

Why transform?

Organizations are modernizing their businesses, processes and products by implementing faster and frequently changing digital technologies. 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 140-2 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.
- **Blockchain.** Widely used for the financial and IoT industries to create smart contracts, issue cryptocurrency, and record transactions, it is imperative for blockchain ledgers to have the tightest security. Reduce risk by using high entropy key generation; implementing strong authentication; and generating, storing and managing keys used to sign the blockchain inside the safe confines of the tamper-proof 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.
- **Bring your own key (BYOK).** 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.

"The more digitally transformed an organization, the more likely that it has experienced a data breach."

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, blockchain, 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 security architecture including side channel attack protection; audit logging; MofN authentication; multi-factor authentication; and separating your HSM into up to 100 partitions each acting as a unique virtual HSM to secure additional applications and extend your return on investment.
3. **Easily and cost-effectively meet your compliance needs** from GDPR and eIDAS to PCI-DSS and CCPA, with the most certifications in the industry including FIPS 140-2, Common Criteria, ITI, 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 quantum-safe 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 with Thales Crypto Command Center.
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 25 years, Thales has been the market leader continuously innovating its high-assurance FIPS 140-2 Level 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 IoT, blockchain, and quantum computing. 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

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.