cpl.thalesgroup.com

THALES
Building a future we can all trust

# Security and Compliance for Cloudera Data Platform

## Using Luna HSM to securely store Cloudera data-at-rest encryption keys

Thales and Cloudera present a high-performing, scalable enterprise-ready big data platform that keeps data-at-rest safe and enterprise customers compliant.

## The problem

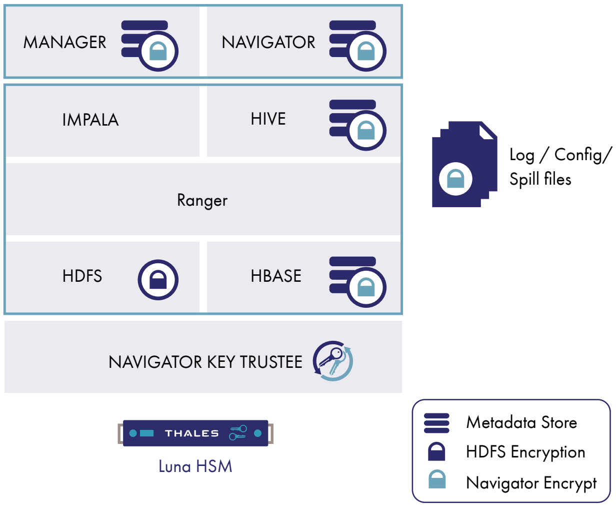
Enterprises of every size are generating more data than ever before. Analysts from IDC to Gartner report that this trend will only accelerate. Enterprises are turning to Cloudera to turn their data into actionable insights that ultimately deliver greater value for the business. With such large quantities of sensitive data involved these organizations must stay diligent in keeping their data safe and staying compliant with their regulatory obligations.

Fortunately, Cloudera and Thales partner to offer a secure way to collect and analyze their data to power the future of their business. Now, customers can secure their data with Cloudera's transparent encryption while securely storing those keys in Thales Luna HSM.

## About Cloudera

Cloudera offers an enterprise data management hub built on the Apache ecosystem of solutions. With Cloudera, enterprises have one place to store, access, process, secure, and analyze their data so they seamlessly use their data to advance their business goals in new and innovative ways. Its open-source big data platform is widely adopted globally, and is supported by their continued contributions to the open source ecosystem.

Cloudera Navigator Key Trustee Server is an integrated part of the Cloudera platform. Key Trustee Server uses industry standard AES-256 encryption as a transparent layer between applications and file systems to secure sensitive data without impacting datacenter performance.



Customers can use Key Trustee Server's automatic deployment and simple configuration to secure data with encryption in minutes instead of days. It also includes process-based access controls that allow authorized processes to access encrypted data while simultaneously preventing administrators or super-users from accessing data outside of their job responsibilities.

Using Thales Luna HSM to secure Cloudera's native encryption keys externally in a hardware appliance ensures that encrypted data is protected from unauthorized access—even as the size of the encryption deployment grows.

Thales Luna Hardware Security Module (HSM) integrates with Cloudera Navigator Key Trustee Server to provide Cloudera encryption keys with both physical and logical security.

## About Thales Luna HSM

Luna HSMs are dedicated devices that are specifically designed to protect cryptographic keys. As a purpose built appliance, Luna HSMs are designed to keep encryption keys within their boundaries and to accept offloaded cryptographic process in order to ensure that keys are never made vulnerable outside of the appliance. Organizations that have strict regulatory requirements for key storage or data sovereignty use HSM technology to assure the integrity of their cryptographic architecture and meet their compliance obligations. Luna HSMs act as trust anchors that protect the cryptographic infrastructure of some of the most security-conscious organizations in the world by securely managing, processing, and storing those keys inside a hardened, tamper-resistant device. Luna HSMs are FIPS 140-2 Level 3 and EAL 4+ Common Criteria validated.

## Benefits

### Seamless encryption of big data implementations

- Transparently and automatically encrypt data with minimal impact on performance or end-user experience

### Satisfy regulators

- Separate encryption keys from encrypted data to follow best practice and meet regulatory obligations
- No rearchitecting required
- No changes to your existing implementation is necessary

### Centralized key management

- Centrally control encryption keys for stronger oversight, more robust security and high scalability
- Granular access controls
- Define and enforce policies to guard against unauthorized and rogue access to, and exposure of, high value data

### Data shredding

- Support compliance mandates, such as HIPAA and PCI DSS, in your big data implementation

Luna HSMs are also available as a service delivered from the Thales cloud. Luna Cloud HSM allows organizations to rent a partition in an HSM without having to rack an appliance in their own data center. For enterprises adopting a cloud first strategy, Luna Cloud HSM is a convenient alternative to the on-premises appliance.

### Address Compliance

Whatever the compliance need, from GDPR and eIDAS to PCI-DSS and CCPA, Luna HSMs are part of the solution. Luna HSMs offer the most certifications in the industry including Common Criteria, FIPS 140-2, ITI and more, and address many common controls related to key storage, data control and data sovereignty.

### Scalable Security for Virtual and Cloud Environments

Separate Thales Luna Network HSMs into up to 100 cryptographically isolated partitions, with each partition acting as if it were an independent HSM. A single Luna HSM can act as the root of trust that protects the cryptographic key lifecycle of hundreds of independent applications, providing you with a tremendous amount of scalability and flexibility. Keys and partitions are cryptographically separated from each other, allowing enterprises and service providers to leverage the same hardware for multiple tenants and appliances. Secure Cloudera native encryption keys in addition to other cryptographic resources in the enterprise.

### Approach to Key Security: Keys in Hardware

Protect keys across their entire lifecycle within the FIPS 140-2 validated confines of the Thales Luna Network HSM. Thales' unique approach to protecting cryptographic keys in hardware positions Luna appliances as the most trusted general purpose HSMs on the market. Unlike other methods of key storage which move keys outside of the HSM into a "trusted layer," the keys-in-hardware approach ensures that your keys always benefit from both physical and logical protections.

## Conclusion

Growing data volumes are an opportunity, not an obstacle. With the right tools, organizations can begin to dream bigger and to do so without risking the privacy of their users' data or the wrath of regulators in their industry. Cloudera and Thales, together, ensure that customers can take advantage of the era of big data without compromising the security of the data on which they depend. To learn more, visit: cpl.thalesgroup.com/Partners/Cloudera

## 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.