

Securing sensitive data in Cloudera

Using Thales KeySecure to securely manage Cloudera Navigator data-at-rest encryption keys



Thales and Cloudera present a high-performing, scalable enterprise-ready Apache Hadoop solution 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 with some postulating that global data volume will reach 40,000 exabytes by the end of next year. Enterprises are turning to Cloudera to turn this data into actionable insights that deliver greater value. With vast quantities of sensitive data involved, and Hadoop's distributed format, customers will need to be diligent in keeping their data safe and meeting their regulatory obligations.

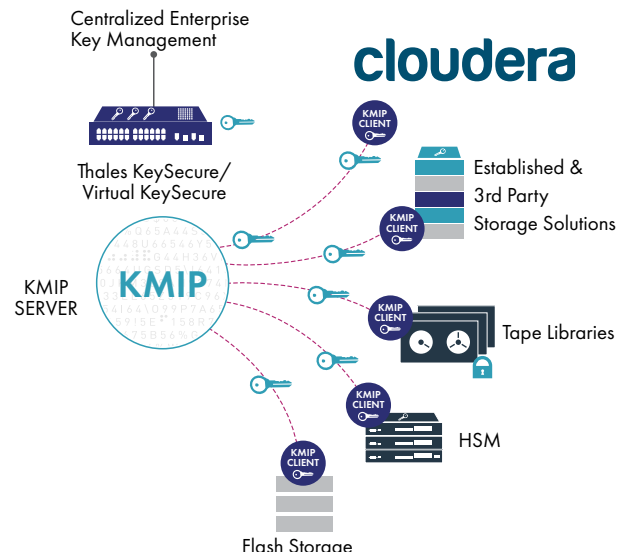
Fortunately, Cloudera and Thales have teamed up to offer enterprises a secure way to implement Hadoop. Now, customers can secure their data with Cloudera Navigator's transparent encryption while storing and managing those keys and associated policies in Thales' KeySecure.

About Cloudera Navigator Encrypt

Cloudera offers an enterprise data management hub built on Apache Hadoop. With Cloudera, enterprises have one place to store, access, process, secure, and analyze all their data so they can extend the value of their existing investments while also deriving

new and innovative value from their data. Its open-source big data platform is widely adopted globally, and is supported by their continued contributions to the open source Hadoop ecosystem.

Cloudera Navigator Encrypt is an integrated part of the Cloudera platform. Navigator Encrypt 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 Cloudera Navigator's automatic deployment and simple configuration to secure data with encryption in minutes instead of days. Navigator Encrypt also includes process-based access controls that allow authorized Hadoop processes to access encrypted data while simultaneously preventing administrators or super-users from accessing data outside of their job responsibilities.

Using Thales KeySecure to centralize encryption key storage not only simplifies key management, but also ensures that encrypted data is protected from unauthorized access—even as the size of the encryption deployment grows.

Thales KeySecure integrates with Cloudera Navigator Encrypt for the hardware storage and management of Cloudera encryption keys, providing robust, enterprise-scale key management, ensuring that keys are managed throughout their lifecycle and properly secured with FIPS 140-2 certified hardware. Thales also offers a hardened virtual security appliance that provides organizations with a more operational—and expense friendly alternative to using a hardware appliance.

About Thales KeySecure

Thales KeySecure is an Enterprise Key Management (EKM) solution that enables a single, centralized platform for managing cryptographic keys and applications. With Thales KeySecure, administrators can simultaneously manage multiple, disparate encryption appliances and associated keys through a single, centralized key management platform.

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

Key features

Duty separation among administrators

Separating administrative duties is an important security best practice that protects data from privileged users and facilitates regulatory compliance. Thales KeySecure's access controls restrict access to encryption keys which in turn can determine data access according to job roles and responsibilities. This flexibility permits Hadoop administrators to be responsible for the Cloudera implementation without ever having access to data in cleartext while security administrators remain solely responsible for the encryption keys.

Compliance made straightforward

Thales protects data at rest to help organizations achieve compliance with regulations governing (including but not limited to) credit card numbers for Payment Card Industry Data Security Standard (PCI DSS) compliance, Personally Identifiable Information (PII) to comply with state data breach and data privacy laws, and Electronic Patient Health Information (EPHI) in accordance with HIPAA. Unifying and centralizing policy management, logging, and auditing makes information more readily accessible and demonstrating compliance with data governance requirements straightforward.

Simplified, consolidated key management

Thales KeySecure centralizes key administration behind an intuitive graphical user interface to make management easy. In addition to managing Cloudera encryption keys, Thales KeySecure's Key Management Interoperability Protocol (KMIP) support allows customers to consolidate and manage keys from a broad ecosystem of partners. Simplified, consolidated key management improves administrative visibility, lessens the chance for error, and reduces the time and effort of managing encryption across the organization.





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.

> cpl.thalesgroup.com <    

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchoi, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: apacsales.cpl@thalesgroup.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com