

CipherTrust Big Data Security



Challenge: protecting private and sensitive data within the Big Data lake

The explosive growth of data in every aspect of our lives and in enterprises around the world has led to growing demand for business intelligence from this data. Enterprises depend on this intelligence to meet the needs of their customers quickly and with precision. However, big data exposes enterprises to numerous data security threats. If an unauthorized user gains access to big data to siphon off and sell valuable information, the losses to the data-holding organization can be severe. Without the right security, big data can pose big security challenges.

Solution: CipherTrust Data Security Platform protection for Big Data environments

The CipherTrust Data Security Platform is an integrated data-centric suite of products that combines data discovery and classification with data protection. The platform makes administration efficient with a “single pane of glass” centralized management console that equips organizations with powerful tools to discover and classify sensitive data, combat external threats, guard against insider abuse, and establish persistent controls across their big data environments—including data sources, infrastructure, and analytics. By delivering a single scalable security platform, Thales helps organizations secure their digital transformation and safely take full advantage of the benefits of big data. The CipherTrust Data Security Platform is composed of an integrated suite of products built on a common, extensible infrastructure with efficient, centralized key and

policy management. As a result, security teams can address data security policies, compliance mandates, and best practices, while reducing administrative effort and total cost of ownership.

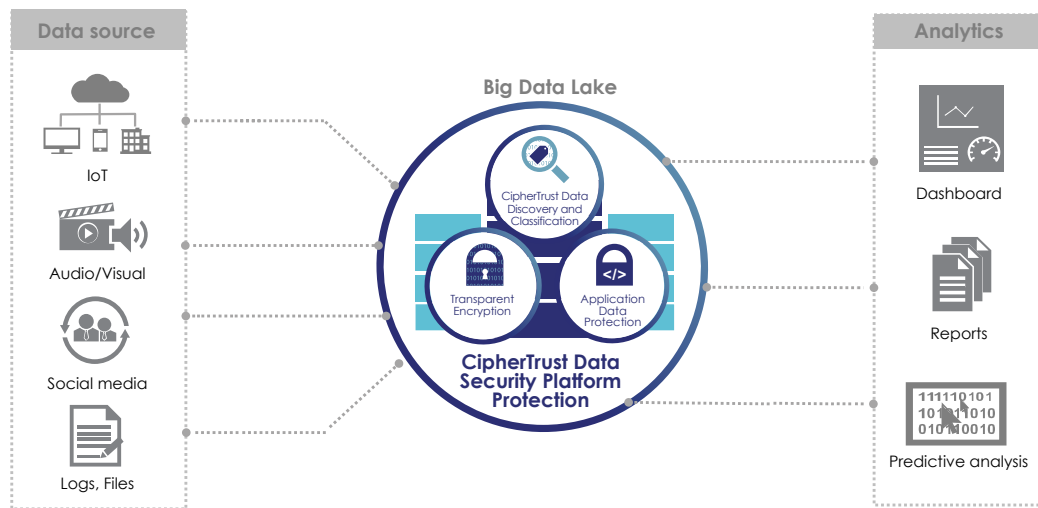
Seamlessly protect Big Data environments

The CipherTrust Data Security Platform enables customers to secure their big data deployments – whether in a Hadoop infrastructure or a non-relational (NoSQL) database, such as MongoDB – to make the most of big data analytics while addressing compliance and regulatory requirements. The extensible platform from Thales is tunable to protect data as granular as specific columns within a relational database or fields within a document, or it can protect all the data within a given directory or volume. The platform supports the broadest range of operating systems and environments in the industry, and it delivers operational efficiencies through the high-performance, centralized CipherTrust Manager.

Benefits

By leveraging the CipherTrust Data Security Platform to secure big data lake environments, your organization can realize the following benefits:

- **Compliance.** The CipherTrust Data Security Platform addresses a broad set of use cases to discover, classify, and protect sensitive data across their big data environments. The platform delivers the comprehensive capabilities that enable organizations to address the demands of evolving regional data protection and privacy laws.



- **Prevent privileged-user threats.** The CipherTrust Data Security Platform provides the fine-grained, policy-based access controls, including Hadoop granular user access controls, which restrict access to encrypted data. These allow only approved access to data by processes and users as required to meet strict compliance requirements.
- **Achieve robust security.** Make the most of big data analytics with confidence that the collected and mined data, including that which is sensitive, is protected.

Features

- **High-performance solutions.** To establish data security in big data environments, organizations can use the following CipherTrust Data Security Platform products:
 - **CipherTrust Data Discovery and Classification** enables organizations to efficiently locate regulated data, both structured and unstructured, within the big data lakes. A single pane of glass delivers understanding of sensitive data and its risks, enabling better decisions about closing security gaps, prioritizing remediation, or securing your cloud transformation and third-party data sharing. The solution provides a streamlined workflow all the way from policy configuration, discovery, and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.
 - **CipherTrust Transparent Encryption** encrypts and controls access at the file-system level to protect structured and unstructured data types from APTs and privileged user abuse. The solution provides the fine-grained, policy-based access controls, including Hadoop granular user access controls, that restrict access to encrypted data. These allow only approved access to data by processes and users as required to meet strict compliance requirements.
- **CipherTrust Application Data Protection** enables developers to easily build encryption for individual fields or specific columns in an application before it writes the field to a database. This ensures that specific fields remain unreadable, even after data is imported into, and processed within, the big data environment.
- **CipherTrust Tokenization** combines the scalability and availability benefits of a protecting data: both format-preserving and random tokenization. Format-preserving tokenization enables data protection without changing database schemas and offers irreversible tokens. Random tokenization offers high performance, convenient data protection.
- **Centralized Key Management.** The centralized management environment provides policy control as well as secure generation, management, and storage of encryption keys. It can enforce strong separation of duties by requiring the assignment of key and policy management to more than one data security administrator.
- **CipherTrust Security Intelligence.** These logs report authorized and unauthorized access attempts to encrypted files and volumes. In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.
- **Simple, non-disruptive implementation.** No development changes are required to existing applications or infrastructure. Scalability for high throughput, high demand environments with easy expansion to protect growing amounts of data.

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.