

Data Protection Solutions for the Databricks Data Intelligence Platform with Thales CipherTrust Manager

Thales helps protect
sensitive information with
defense-in-depth offerings

To complement the robust security of the Databricks Data Intelligence Platform and offer users advanced security options for sensitive information, Thales collaborates with Databricks on various technical integrations and solution offerings to enhance organizations' defense-in-depth strategies.

The Databricks Data Intelligence Platform is a unified platform that connects organizations to essential data and applications globally, breaking down internal silos and enabling seamless collaboration. Powered by a unique architecture, it integrates data and workloads at any scale, simplifying data management and maximizing value extraction.

While Databricks already provides strong built-in data protection capabilities, organizations handling sensitive data often choose external data protection and key management solutions, such as Thales, for various business and technical reasons.

Thales Data Protection Solutions for Databricks

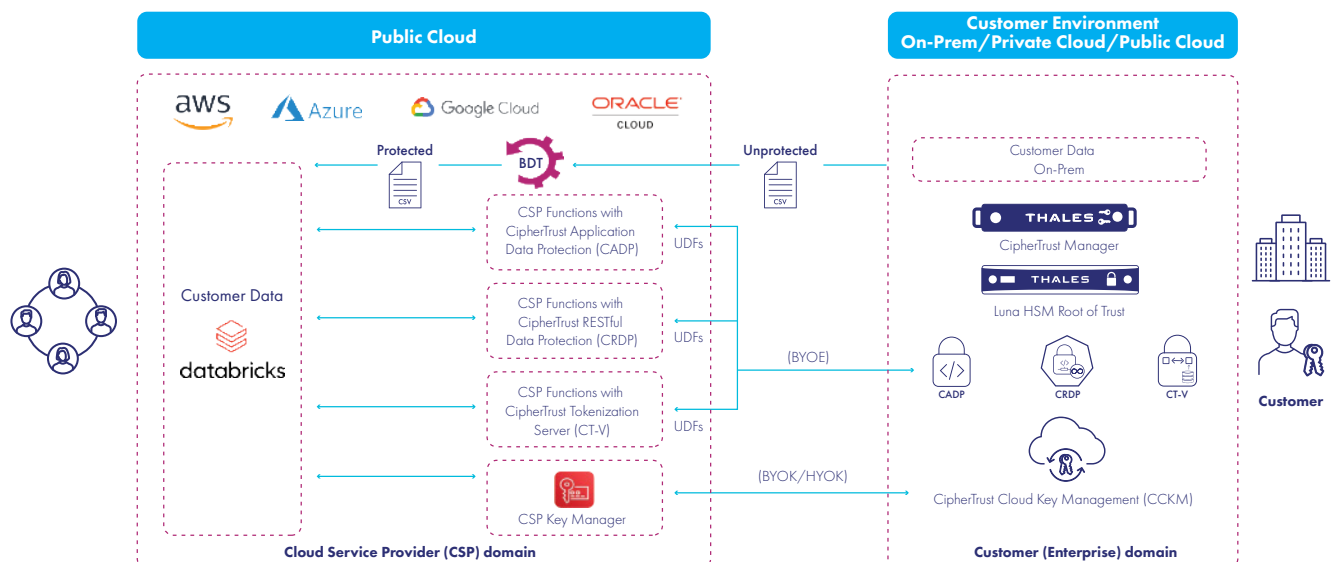
To improve data protection, facilitate regulatory compliance, and empower user choices, Thales solutions can be deployed for the Databricks Data Intelligence Platform, either independently or in combination with one another.

The Thales CipherTrust Data Security Platform (CDSP) provides users with several enhanced security and data protection measures for their Databricks deployments, including Bring Your Own Encryption (BYOE), Bring Your Own Key (BYOK), and Hold Your Own Key (HYOK). Thales CipherTrust Manager (CM), the centralized management point for the CDSP platform, delivers an industry-leading enterprise key management solution. It allows organizations to manage encryption keys centrally, provide granular access control, and configure security policies. CM is available in virtual and physical form factors and can leverage embedded Luna Network HSMs or select cloud HSMs to enable FIPs 140-3 Level 3 highest level root of trust.

Bring Your Own Encryption (BYOE) Encryption / Tokenization

Thales CipherTrust provides a comprehensive range of Bring Your Own Encryption (BYOE) solutions to organizations utilizing the Databricks Data Intelligence Platform. These solutions include encryption, tokenization, data generalization, static data masking, dynamic data masking and redaction. Data types requiring protection may include credit cards, social security numbers, driver licenses, passport numbers, and national identity numbers. Sensitive data is transformed, making it unreadable or unusable to prevent the misuse of such information. BYOE is regarded as the highest level of protection when it comes to encryption since the user owns the encryption/tokenization and the associated keys. As an external encryption and tokenization partner to Databricks, CipherTrust RESTful Data Protection, CipherTrust Application Data Protection and CipherTrust Vaulted Tokenization are BYOE solutions that enable the use of Databricks remote external functions and user-defined functions.

Protecting Sensitive Data in Databricks Data Intelligence Platform



External Key Management: Bring Your Own Key (BYOK) / Hold Your Own Key (HYOK)

Industry best practices and compliance mandates, such as the SCHREMS II ruling on digital sovereignty, require organizations to maintain control over their encryption keys. This control is especially crucial for organizations relying on cloud-based or Software-as-a-Service (SaaS) solutions. Although data may physically reside in the Databricks Data Intelligence Platform, an organization that retains logical key control ultimately maintains authority over its sensitive data. The entity holding the keys can dictate who has access to view and utilize the information.

Thales CipherTrust Cloud Key Manager (CCKM) can operate alongside a Databricks-maintained key management system to create a composite master key for data protection. CCKM enables Databricks users to create and manage their encryption keys using Bring Your Own Key (BYOK) in a FIPS-certified appliance, which remains entirely under their control. Furthermore, CCKM allows users to externally store and manage the keys used to encrypt their data, utilizing Hold Your Own Key (HYOK) in relation to the Databricks Data Intelligence Platform in a virtual or physical appliance. By controlling the keys, users can separate, create, own, manage, and control, including the revocation of encryption keys and tenant secrets used to create them.

Business Highlights for Customers

Defense in Depth - Thales provides robust third-party security and data protection solutions for Databricks users seeking to safeguard sensitive information. These layered protections are available across virtual and physical deployments and can be utilized in multi-cloud and hybrid cloud environments, ensuring user choice.

Supports Data Sovereignty Requirements - Thales guarantees that Databricks users can securely store and manage encryption keys. This strategy addresses several key privacy and data sovereignty requirements organizations encounter while simplifying the process of demonstrating compliance to regulators.

Meets Compliance Mandates - Thales provides a unified management console, making it easier to discover and classify data and meet increasingly stringent data protection compliance mandates like PCI DSS, GDPR, and CCPA.

About Databricks

Databricks is the Data and AI company. More than 10,000 organizations worldwide — including Block, Comcast, Condé Nast, Rivian, Shell and over 60% of the Fortune 500 — rely on the Databricks Data Intelligence Platform to take control of their data and put it to work with AI. Databricks is headquartered in San Francisco, with offices around the globe and was founded by the original creators of Lakehouse, Apache Spark™, Delta Lake and MLflow. To learn more, follow Databricks on X, LinkedIn and Facebook.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.