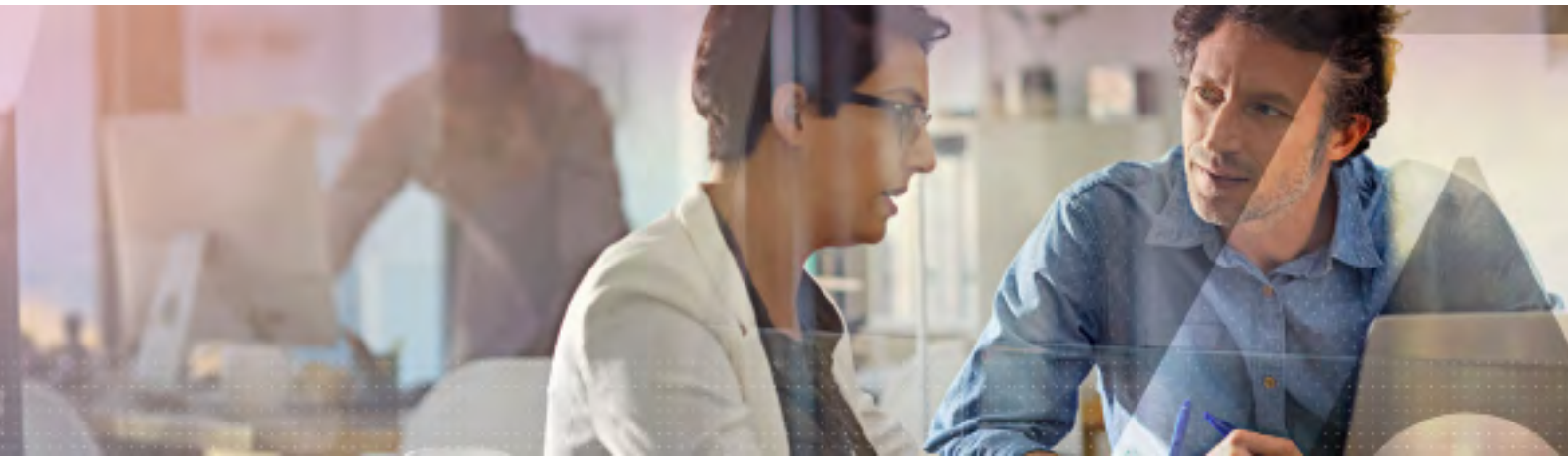
cpl.thalesgroup.com

THALES

Security and Compliance for Confluent Kafka

Thales Ciphertrust Transparent Encryption For Confluent Kafka



Key Benefits

- Robust file-system-level data encryption
- Administrative simplicity
- Granular privileged user access policy enforcement
- Comprehensive compliance controls and audit trails

The Problem: Sensitive Data Needs Protection

Organizations adopt Confluent Kafka to simplify the interconnectivity of their applications and the flow of data throughout their organization. While this streaming data renders technical operations more efficient and effective, it also becomes highly attractive to those seeking to steal or compromise the data. Amid all of these operational and security considerations, these organizations must also consider their compliance obligations many of which detail how data must be kept secured from unauthorized users.

The Challenge: Security And Compliance Needs To Be Efficiently Met

Organizations risk exposing themselves to fraud and data breaches when they implement insufficient security controls. For example, without a form of encryption or tokenization, Confluent Kafka Platform administrators can have control of both the Kafka environment and the data that flows through it. By design, Kafka

centrally aggregates data, which presents a tempting target for thieves. This data can vary widely and include sensitive, regulated resources, like customer payment data, patient records and intellectual property. If Kafka data is not properly secured, there is potential for insider abuse. Any organization adopting Confluent Kafka will also need to think about how they keep their data secure.

Fortunately, Confluent and Thales work together to solve these security and compliance concerns.

The Solution

CipherTrust Transparent Encryption (CTE) secures data at-rest in Confluent Kafka with file system-level encryption backed by centralized key management, privileged user access controls and detailed data access audit logging. CTE protects data wherever Kafka broker nodes reside, on-premises and across clouds.

CTE deployment is quick, simple, and scalable; agents are installed at the operating file-system or device layer on servers running Kafka broker nodes. Administrators set policies for the directories that need protection, and any data written to or read from those locations will automatically be encrypted or decrypted. Encryption and decryption is transparent to all applications streaming data to Kafka meaning that CTE addresses compliance obligations and data security best practice requirements in real time with minimal disruption and effort. CTE's implementation is seamless and keeps both business and operational processes working without changes even during deployment and roll out. CTE works in conjunction with the FIPS 140-2 up to Level 3 validated Data Security Manager, which centralizes encryption key and policy management for the CipherTrust Data Security Platform.

Why Use Thales Ciphertrust Transparent Encryption With Confluent Kafka?

When customers use Confluent Kafka with CTE, they can accelerate their application development with confidence knowing that their highly-sensitive regulated data is safe, and that they are addressing their compliance obligations for securing data at rest. Customers can use Thales' centralized key management to incorporate Confluent Kafka encryption efficiently into their larger organizational security strategy. By using privileged user access controls and detailed data access audit logging, customers separate security and administrative platform duties between administrators in a way that increases visibility of the data's security – both improving the data's safety and satisfying key compliance requirements.

Administrative Simplicity

CipherTrust Transparent Encryption minimizes the time and effort needed to implement and maintain data encryption. CTE file encryption secures data without requiring code changes to the Confluent Kafka Platform or any associated applications. Furthermore, the underlying Data Security Manager provides a unified, centralized platform to manage data-at-rest encryption keys and policies across an enterprise's storage, databases and applications.

Granular Privileged User Access Policy Enforcement

Security teams can use CTE to establish and enforce granular, least-privileged user access policies (e.g. by user, process, file type, time of day) to data on the Confluent Kafka Platform. Security admins use these policies to grant specific users access to clear-text data, and to limit the file system commands that they can perform. These access controls establish a layer of separation between systems and data that increases security and visibility of access to the data. In this way, security teams can permit platform administrators to manage configurations and ongoing maintenance on the Confluent Kafka Platform without having clear-text access to the sensitive data that resides within.

Comprehensive Compliance Controls and Audit Trails

CTE delivers detailed data access audit logs to address many general compliance and regulation controls relating to encryption, data sovereignty, least-privileged policy and data access auditing. Auditors use intelligence logs to assess encryption, key management and access policy effectiveness. Logs also reveal when users and processes access data, under which policies, whether requests were allowed, and even when a privileged user submits a command like "switch user" to attempt to imitate another user. Additionally, CTE's pre-built integration to leading Security Information and Event Management (SIEM) systems mean the log data is immediately actionable.

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.

About Confluent

Confluent, founded by the original creators of Apache Kafka®, pioneered the enterprise-ready event streaming platform. With Confluent, organizations benefit from the first event streaming platform built for the enterprise with the ease of use, scalability, security, and flexibility required by the most discerning global companies to run their business in real time. Companies leading their respective industries have realized success with this new platform paradigm to transform their architectures to streaming from batch processing, spanning on-premises and multi-cloud environments.

For more detailed technical specifications, please visit https://cpl.thalesgroup.com/ or https://www.confluent.io/