

External Key Management for EDB Postgres AI with **Thales CipherTrust Manager**

Securely store and manage encryption keys to meet security and regulatory needs

The Challenge

Data is an organization's most precious asset. While encryption is a key tool for securing data, it is not the answer alone. When encryption keys are improperly stored or managed, encrypted data is at risk from anyone, from hackers to privileged administrators, who improperly access the related keys. Perhaps more important than encryption is the key management used to support it. Data is often regulated, requiring external key management as a security measure. These regulations require detailed logging and access information for compliance, which encryption alone cannot provide, risking hefty fines. In short, organizations must secure their data to satisfy regulators and leave organizations in sole control. Enterprise DB (EDB) has given the first level of tools required to meet these goals.

Organizations choose EDB Postgres AI for the performance, reliability, and manageability features it brings to make open-source projects suitable for enterprise-level workloads. Along with its monitoring, optimization, CLI migration tools, Kubernetes, and container support, EDB has developed its own encryption functionality to enhance the open-source offering. Transparent Data Encryption (TDE) is a cornerstone of database encryption, offering file-level encryption. It aims to protect organizations and their customers' data from various security risks.

The Solution

Thales CipherTrust Manager is an enterprise key management platform that allows customers to securely store their EDB encryption keys externally from the database server, protecting the keys if the server is ever compromised. It is available in a physical, virtual, and as-a-service model to fit a wide range of organizational security and budgetary approaches. With a broad ecosystem of key management partners, CipherTrust Manager is FIPS 140-2 certified and lets customers store and manage their EDB TDE keys alongside keys from other third-party solutions and Thales' CipherTrust Data Security encryption and tokenization solutions.

Benefits

Satisfy Data Privacy and Security Regulations

Sensitive data is often regulated by industry and government regulations stipulating encryption and external key management. CipherTrust Manager allows customers to demonstrate control of their data and comply with requirements laid out in regulations and standards such as PCI DSS, NYDFS, GDPR, DORA and LGPD. Adhering to these regulations becomes more complicated as organizations adopt cloud-based or AI technologies that can contain sensitive data. With CipherTrust Manager and EDB, organizations can clear these obstacles and unlock innovation using the most advanced and scalable tools.

Save Time, Money, and Effort

Consolidating key management to one platform, CipherTrust Manager recovers the budget spent on solutions from multiple vendors, saves time associated with managing multiple solutions, and frees up valuable staff time to focus on more important projects. Additionally, with an ongoing shortage of skilled IT security practitioners, centralizing key management saves time and streamlines workflows when managing complicated, large-scale cryptographic landscapes.

Improved Security from Detailed Auditing and Reporting

CipherTrust Manager tracks all key state changes, administrator access, and policy changes in various log formats, making integration into an organization's SIEM tools easy. Centralizing key management with CipherTrust Manager improves security by providing additional visibility and simplification. This reduces the room for human error and provides greater data and insight into how EDB TDE keys are used and who is accessing them.



Key Management



Access Policies



Auditing Reporting



Flexible APIs



CipherTrust Manager

Conclusion

EDB keeps an organization's most sensitive data safe against would-be attackers. It facilitates migrations from Oracle Database, where organizations are accustomed to TDE security. It opens the door to incorporating sensitive data in AI by addressing the regulatory barriers inhibiting adoption today. With Thales CipherTrust Manager, EDB Postgres AI has the accompanying key management tool needed to achieve these gains fully and more, ultimately making EDB fully adoptable by large-scale enterprises.

About EDB

EDB provides a data and AI platform that enables organizations to harness the full power of Postgres for transactional, analytical, and AI workloads across any cloud, anywhere. EDB empowers enterprises to control risk, manage costs and scale efficiently for a data and AI-led world. Serving more than 1,500 customers globally and as the leading contributor to the vibrant and fast-growing PostgreSQL community, EDB supports major government organizations, financial services, media and information technology companies.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.