Solution Brief

Security and Compliance for Postgres Database

Thales Database Encryption for EDB Postgres AI

cpl.thalesgroup.com

THALES
Building a future we can all trust

EDB POSTGRES AI

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

EDB Postgres® AI combines open-source PostgreSQL with enterprise features to reduce risk and complexity. Key functionalities include performance diagnostics, Oracle® database compatibility, and tools for developer and DBA productivity. Organizations adopt EDB Postgres AI to build their AI on their terms with a data platform they control, enabling agentic AI ambitions for hybrid deployments. As the root to an increasing number of applications, organizations are storing highly sensitive, regulated data in their EDB Postgres AI databases – data that needs protection from malicious insiders and external attackers.

The Challenge: Security and Compliance Needs to be Efficiently Met

Insufficient security controls expose your organization to fraud and data breaches. For example, when security is handled within the database, the DBA can have control of both the database and cleartext data. Databases, by design, centrally aggregate data, and in turn, present a focal point for thieves. This data can vary widely and include sensitive, regulated resources, like customer payment data, patient records and intellectual property. If the database is not handled or configured correctly, there is potential for insider abuse, as well as advanced persistent threats, where an attacker imitates a privileged user. Any organization adopting EDB Postgres AI also needs to consider how they are securing their data.

Fortunately, EDB Postgres AI and Thales team together to address this security and compliance concern.

CipherTrust Transparent Encryption for EDB Postgres AI

The solution

CipherTrust Transparent Encryption secures data at-rest in EDB Postgres AI with file system-level encryption backed by centralized key management, privileged user access controls and detailed data access audit logging. CipherTrust Transparent Encryption protects data wherever EDB Postgres AI resides, on premises, across clouds and within container environments. CipherTrust Transparent Encryption deployment is simple, scalable and fast, with agents installed at the operating file-system or device layer wherever EDB Postgres AI is installed. Encryption and decryption is transparent to the database and all applications that run above it. CipherTrust Transparent Encryption addresses data security compliance and best practice requirements with minimal disruption, effort, and cost. CipherTrust Transparent Encryption's implementation is seamless and keeps both business and operational processes working without changes even during deployment and roll out. CipherTrust Transparent Encryption works in conjunction with the FIPS 140-2 up to Level 3 validated CipherTrust Manager, which centralizes encryption key and policy management for the CipherTrust Data Security Platform.

Why use Thales CipherTrust Transparent Encryption with EDB Postgres AI?

When customers use EDB Postgres AI with CipherTrust Transparent Encryption, they can confidently build new applications or migrate legacy systems to Postgres knowing that their highly-sensitive regulated data is safe, and that they are addressing their compliance obligations for securing data-at-rest. Using Thales' centralized key management, customers can efficiently incorporate EDB Postgres AI into their larger organizational security strategy. Privileged user access controls and detailed data access audit logging allow customers to separate security and administrative database duties between teams and increase 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. CipherTrust Transparent Encryption file encryption secures data without requiring code changes to the database or any associated applications. Furthermore, the underlying CipherTrust Manager provides a unified, centralized platform to manage dataat-rest encryption keys and policies across an enterprise's storage, databases and applications.

Granular Privileged User Access Policy Enforcement

Security teams can use CipherTrust Transparent Encryption to establish and enforce granular, least-privileged user access policies (e.g. by user, process, file type, time of day) to the EDB Postgres AI. 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 database administrators to manage configurations and ongoing maintenance on EDB Postgres AI without having clear-text access to the sensitive data that resides within.

Comprehensive Compliance Controls and Audit Trails

CipherTrust Transparent Encryption 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, CipherTrust Transparent Encryption's pre-built integration to leading Security Information and Event Management (SIEM) systems mean the log data is immediately actionable.

About EDB Postgres AI

EDB Postgres® AI (EDB PG AI) is the first open, enterprise-grade sovereign data and AI platform—secure, compliant, and scalable, on-premises and across clouds. Built on Postgres, the world's leading database, EDB PG AI unifies transactional, analytical, and AI workloads, enabling organizations to operationalize their data and LLMs while maintaining control over sovereign environments. EDB PG AI is supported by a global partner network and delivers up to 99.999% availability as well as hybrid management and a built-in AI factory. As one of the most active contributors to the PostgreSQL project, EDB is deeply invested in the vitality of the global community. To learn more, visit www.enterprisedb.com.

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.

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us