

Security and Compliance for Postgres Database

Thales Database Encryption for EnterpriseDB Postgres Advanced Server



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

EnterpriseDB® (EDB™) Postgres Advanced Server combines the open-source PostgreSQL with enterprise features to reduce risk and complexity with functionality such as performance diagnostics, Oracle® database compatibility, and developer and DBA productivity features. Organizations adopt EDB Postgres Advanced Server when they modernize legacy applications, develop new applications or migrate from a legacy database. As the root to an increasing number of applications, organizations are storing highly sensitive, regulated data in their EDB Postgres Advanced Server 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 Advanced Server will also need to think about how they are securing their data.

Fortunately, EnterpriseDB and Thales team together to address this security and compliance concern.

CipherTrust Transparent Encryption for EnterpriseDB

The solution

CipherTrust Transparent Encryption secures data at-rest in EnterpriseDB Postgres Advanced Server 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 Postgres Advanced Server 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 Advanced Server 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 Security Manager, which centralizes encryption key and policy management for the CipherTrust Data Security Platform.

Why use Thales CipherTrust Transparent Encryption with EnterpriseDB Postgres Advanced Server?

When customers use EnterpriseDB Postgres Advanced Server 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 EnterpriseDB Postgres Advanced Server 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 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 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 Advanced Server. 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's Postgres Advanced Server databases 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.

EnterpriseDB





EnterpriseDB (EDB), the enterprise Postgres company, delivers an open source-based data management platform, optimized for greater scalability, security, and reliability. EDB Postgres makes organizations smarter while reducing risk and complexity with enterprise-proven management tools, security enhancements and Oracle compatibility. Over 4,000 customers worldwide deploy diverse workloads including transaction processing, data warehousing, customer analytics and web-based applications, both on-premises and in the cloud.

For more detailed technical specifications, please visit cpl.thalesgroup.com or www.enterprisedb.com.

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.

> cpl.thalesgroup.com <    

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us