cpl.thalesgroup.com

THALES
Building a future we can all trust

Achieve Data Security and PCI DSS Compliance for EDB Postgres Advanced Server and Postgres Database with Thales

Introduction

Consumers' payment data is among the most valuable data a company possesses and presents a compelling target for criminals. Increasingly, criminals are finding success in targeting organizations that collect this data. As of the 2019 Thales Data Threat Report – Financial Services Edition 1, 62% of U.S. financial services organizations said they had been breached at some point in their history, with 41% breached in the previous 12 months. Nearly every major financial institution, retailer, and many payment processors have suffered a data breach. EnterpriseDB's Postgres Advanced Server has significant adoption in these spaces which means that it, and the data it holds, are now prime targets for these criminals.

Because this data is valuable, it is also regulated by both government and industry regulations and standards. Any business that wishes to store, process or transmit payment card information must comply with Payment Card Industry Data Security Standard (PCI DSS). Let's take a look at PCI DSS 3.2.1's core requirements for securing sensitive cardholder data, and examines how Thales' encryption, key management, and access control portfolio address them.

Why Data Security?

With organizations orienting their operations around the extraction of value from data, criminals equally see data as a valuable resource. Insufficient security controls expose organizations to fraud and data breaches. 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. 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.

Now, effective security looks to attach protection directly to the data itself. Encryption, and corresponding encryption key management, can keep data safe even if attackers find a way to bypass an organization's firewall. Any organization adopting EDB Postgres Advanced Server will also need to think about how they are securing their data.

Purpose of PCI Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security controls designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

PCI DSS' goal is to protect cardholder and sensitive authentication data wherever it is stored, processed or transmitted. The security controls and processes required by PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. It also applies to all entities that store, process, or transmit cardholder data and/or sensitive authentication data

Thales CipherTrust Transparent Encryption and EDB—the Solution

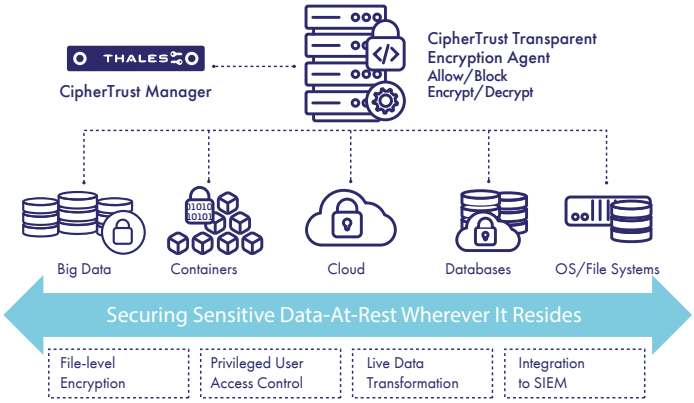
Encryption is the process through which data is encoded so that it remains hidden from or inaccessible to unauthorized users. It helps protect private information, sensitive data, and can enhance the security of communication between client applications and servers. In simple terms, when data is encrypted, even if an unauthorized person or entity gains access to it, they will not be able to read it. Encryption paired with external key management is a highly effective way to protect data and address PCI DSS compliance.

CipherTrust Transparent Encryption secures data at-rest in EDB 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. Thales' portfolio of data protection products includes key management, tokenization, application encryption, and the payment and general purpose hardware security module (HSM) all of which can combine to address an organizations PCI DSS requirements. In addition, Thales offers products that deliver centralized authentication access control functionality.

Database Encryption with CipherTrust Transparent Encryption

CipherTrust Transparent Encryption is an agent based solution that encrypts database data-at-rest at the OS/File-system-level. Customers define which directories they want encrypted, and the agent will encrypt/decrypt read and write operations to that directory. Undefined directories are left alone. These operations do not impact the user experience and are fully transparent to both the application and the database, meaning that there are no required architecture changes to secure data. Customers can also establish policy-based access controls to more narrowly tailor authorized access to the data.

CipherTrust Transparent Encryption encrypts data across multiple clouds, big-data, and container environments. CipherTrust Transparent Encryption is designed to meet PCI DSS requirements and best practices with minimal disruption, effort, and cost.



Note
EBD Postgres Extended represents EBD Postgres-BDR (Bi-Directional Replication) and Barman.

CipherTrust Transparent Encryption has been certified with EDB Postgres Advanced Server, and with EDB Postgres Extended as part of a BDR (bi-directional replication) cluster, and with Barman.

External Key Management with CipherTrust Manager

Thales' CipherTrust Transparent Encryption work in tandem with the CipherTrust Manager external key manager. CTE uses the encryption keys stored on the CipherTrust Manager to perform the encryption/decryption operations on the secured data. CipherTrust Manager centralizes key lifecycle management and user/group-based policy control of encryption keys in one location to streamline administration and centralize oversight via a web-based console, CLI, SOAP, or REST APIs.

CipherTrust Manager is available as FIPS 140-2 Level 3 and Common Criteria EAL4+ certified configurations. CipherTrust Manager's external key management satisfies PCI DSS' requirements for external encryption key storage and management.

CipherTrust Transparent Encryption Benefits

- **Granular Privileged User Access Policy Enforcement**
  Security teams can use CipherTrust Transparent Encryption to establish and enforce granular, least-privileged user access controls (e.g. by user, process, file type, time of day) to the EDB Postgres Advanced Server. These policies grant specific users access to clear-text data, and limit the file system commands that they can perform. In this way, security teams can permit database administrators to manage configurations and ongoing maintenance on EDB's Postgres Advanced Servers without having clear-text access to the sensitive data that resides within.
- **Comprehensive Compliance Controls and Audit Trails**
  CipherTrust Transparent Encryption records detailed data access information in audit logs that organizations can use to demonstrate their PCI DSS compliance. Auditors can use these intelligence logs to assess encryption, key management and access policy effectiveness. Logs 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".

Conclusion

EDB's collaboration with Thales brings industry leading security to our joint customer conversations. Thales CipherTrust Transparent Encryption and CipherTrust Manager fulfill core PCI DSS requirements and can help customers deploy Postgres to collect, transmit and store sensitive payment data. When customers use EDB 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 EDB Postgres Advanced Server into their larger organizational security strategy. And, because they bring a platform approach to the conversation, Thales' CipherTrust Transparent Encryption can help EDB customers satisfy other non-PCI DSS compliance or security requirements.

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 EDB

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.