EDB
Postgres for the AI Generation

Preparing for DORA:
Strengthening Financial Data Security
with EDB Postgres
and Transparent Data Encryption

Gianni Ciolli
Global VP, Practice Lead High Availability
3 December 2024

Gianni Ciolli

- Global VP, Practice Lead HA

- Founder of **2ndQuadrant**

- Author of the **PostgreSQL Administration Cookbook**

- Contributor to PostgreSQL (**Hot Standby**) and related tools such as **PGD**, **Barman**, **TPA**, **repmgr**

Agenda

1. What problem are we trying to solve?

2. Transparent Data Encryption in Postgres

3. Demo

What problem are we trying to solve?

Digital Operational Resilience Act

- EU Regulation

  - Entered into force in 2023

  - Will apply on 17 January 2025

- Goals:

  - Strenghten ICT Security of financial entities

  - Ensure resilience of financial sector in Europe
   in the event of a severe operational digital disruption

What about Postgres and EDB?

- One of the DORA requirements:
  data is **encrypted at rest**

- Addressed by **Transparent Data Encryption** (TDE)

- Feature of **EDB Postgres Advanced Server** (EPAS)

The topic for this webinar

- Info on DORA: <u>https://trust.enterprisedb.com/</u>

- From now on, this webinar will cover **TDE** with **EDB Postgres Advanced Server**
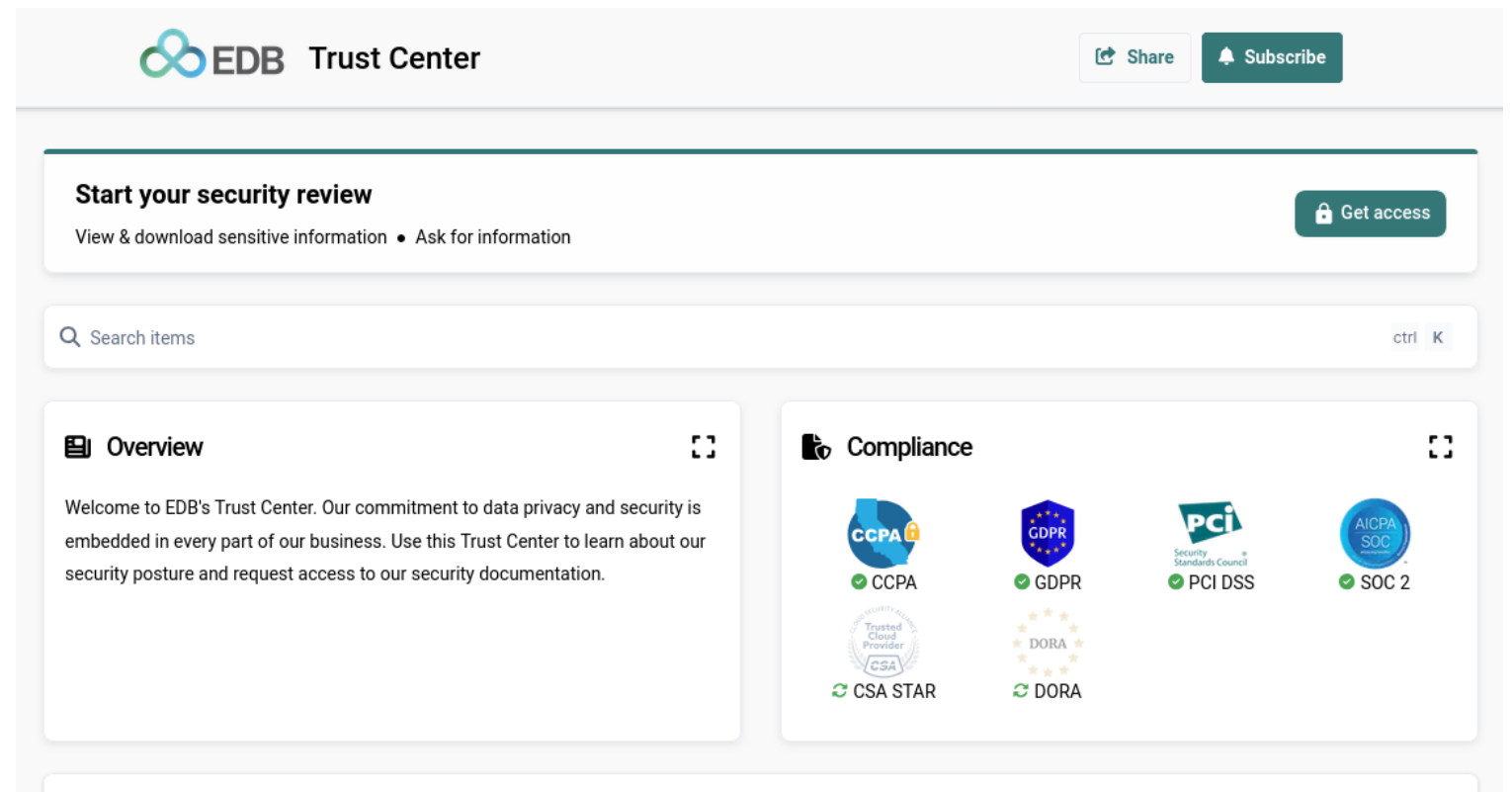
"Why do we need Transparent Data Encryption?
Our disks are already encrypted…"

*"Why do we need Transparent Data Encryption?
Our disks are already encrypted…"*

(will be answered later)

Demo #1: Postgres Data Files

Transparent **D**ata
Encryption in Postgres

TDE Overview

Unencrypted in Memory
Shared Buffers
8k 8k 8k

Remote Host
App

XTS-AES
encrypt/decrypt

Master Encryption Key

Encrypted on Disk
8k 8k 8k
WAL Temp
Data Blocks on Disk

cUEax0Xtnc5CFwEP/051NBb
uFNF3ySC6b3qDbkb+Jo+I73
WclUS1bjrYoCImE0ugAzKWj/
e8PRWaTclw1uAB+uk=

Database File contents unintelligible
Even to system administrators
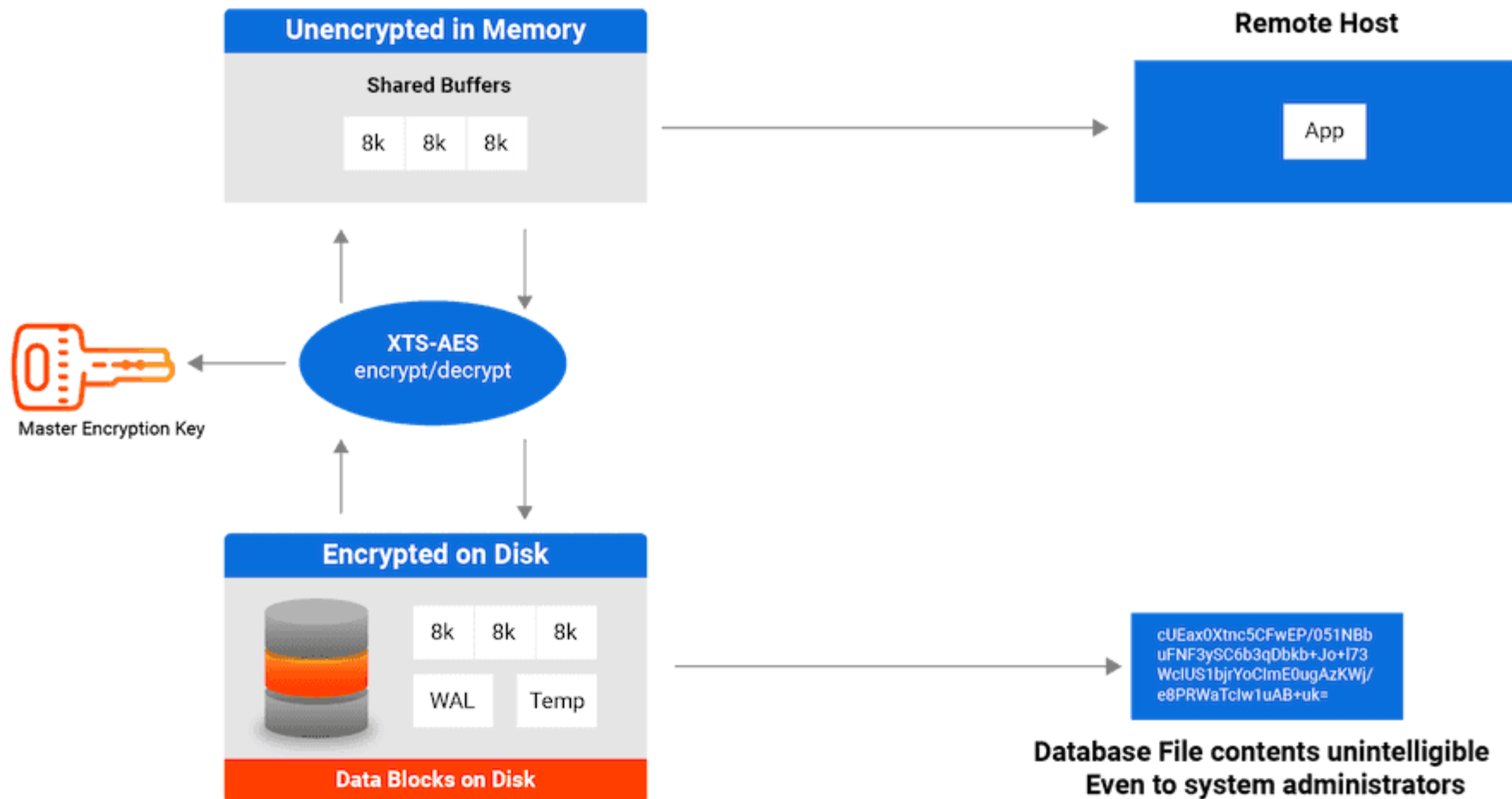
The Two TDE Keys

- The **Data key** is used to encrypt/decrypt data files

- The **Master Key** is used to encrypt/decrypt *(wrap/unwrap)* the Data Key

  - Stored in a Key Store software, not in the database!

  - Postgres retrieves the master key from the Key Store

- Allows *key rotation* without re-encrypting the entire db!

The Key Store

- Software for managing life cycle of master keys
- EDB partners: Thales CypherTrust Manager, Hashicorp Vault
- Examples:
  - Key generation
  - Key rotation
  - Key destruction
  - Key import/export
  - Role-based access control

*"Why do we need Transparent Data Encryption?
Our disks are already encrypted..."*

TDE v Disk Encryption

- With TDE, the data is encrypted at **database level**

- Backup files are encrypted too

  - Can be stored in the cloud without leaking data

  - Reduces surface for security attacks

Demo #2: Transparent Data Encryption

What about performance?

- See the blog article linked from the main TDE docs:
https://www.enterprisedb.com/docs/tde/latest/

"The benchmarks described in this article indicate that the use of EDB's TDE extension does not have a significant impact on transaction performance (<7.5%) or database upgrade times (0.3%)."

Try Out Our Extreme HA Solution

Test drive EDB's five 9s uptime-capable solution with 5x throughput performance.

Start a Free Trial

Continue Your Research

Learn more about how DORA is impacting the future of database resiliency in financial services.

Read the Blog

Access EDB's Security Docs

Learn more about EDB's data security commitment and view our security documentation.

EDB Trust Center

Thank You!

Contact us for your own custom Postgres tools and tuning solutions.