Unlocking security by encrypting your PostgreSQL

Status and story of pg_tde

News flash

Out of the top popular databases PostgreSQL is the only one that does not have TDE

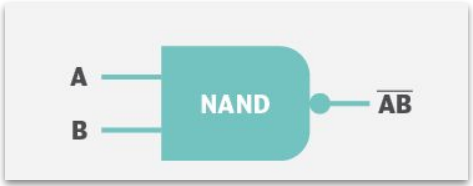
… well not an open source one at least
(as proprietary closed source solutions with TDE based on PostgreSQL exist)

Rank			DBMS
May 2025	Apr 2025	May 2024	
1.	1.	1.	Oracle
2.	2.	2.	MySQL
3.	3.	3.	Microsoft SQL Server
4.	4.	4.	PostgreSQL
5.	5.	5.	MongoDB

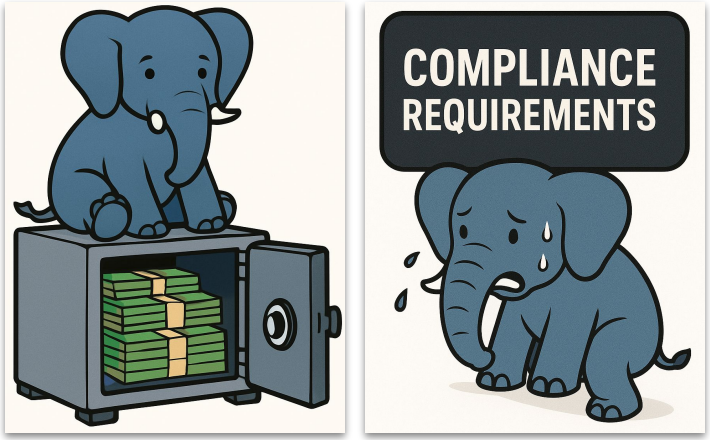
Source DB-Engines Ranking

So what, I can encrypt my filesystem, you may say…

You **may** and in some scenarios you **should**.



Typically we find it more of an **AND** than an **OR** case



Regulators compliance is a demanding set of requirements

PCI DSS 4.0 - example of compliance requirements

Payment Card Industry Data Security Standard

PCI DSS v4.0 – Requirement 3.5.1.2

If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows:

On removable electronic media

OR

If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.

disk encryption can't be **the only means** of rendering cardholder data unreadable.

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Applicability Notes

While disk encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices.

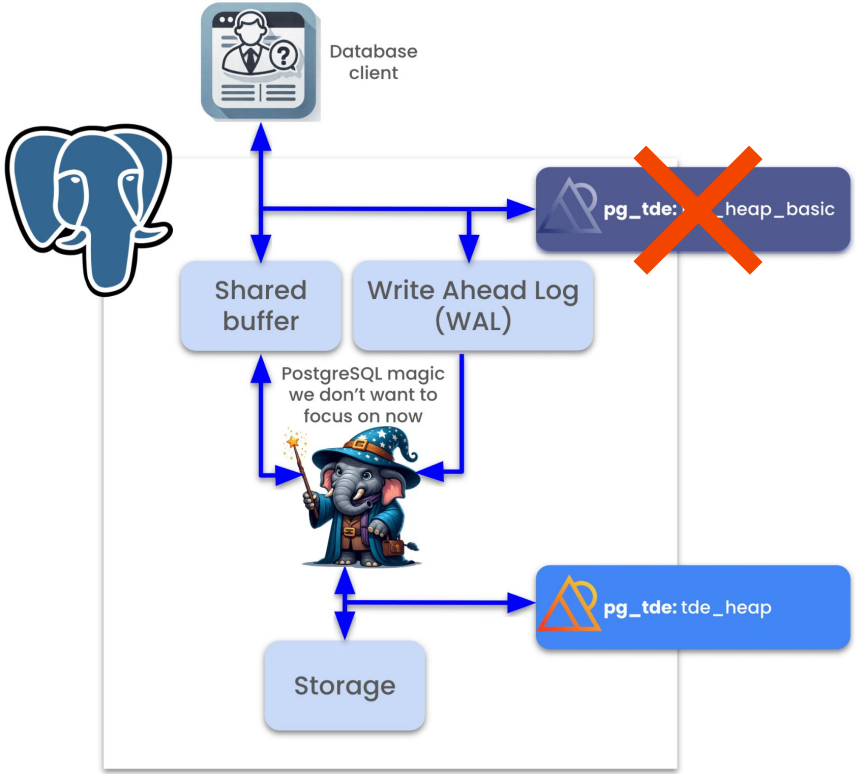
Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies.

Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.

Yes, that's (among others) TDE

So how do we fix it?

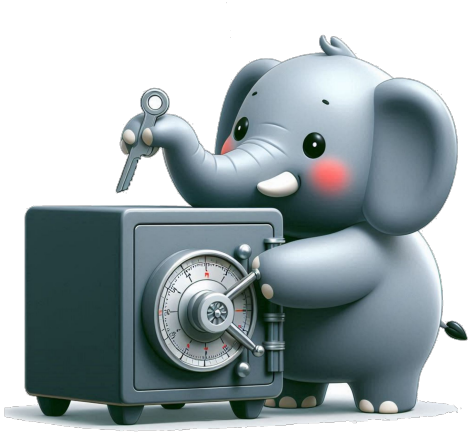
So how do we fix it?



What's included?

Planned for GA

- GA Scope:
  - Extensibility points in PostgreSQL Server
    - Contributed to PostgreSQL Community
  - Fully open source extension
    - Multi-tenant support in envelope encryption model
    - Online data encryption on table level granularity
    - Indexes encryption for the encrypted tables
    - Encryption enforcement
    - KMS integration (KMIP, Secrets Engine kv2)
    - Online key rotation
- Beta feature(s)
  - WAL encryption (Beta)



RC2 is out next week!

Progress report on pg_tde - GA extension is nearer every day!

*May 8, 2025 by **Jan Wieremjewicz***

Another week, another blogpost about the state of open source Transparent Data Encryption (TDE) for PostgreSQL.

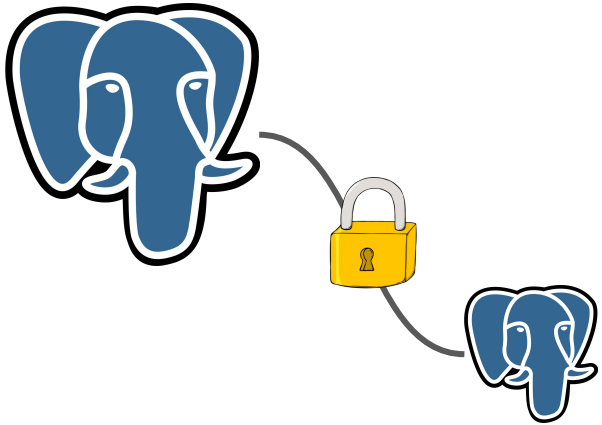
First off, thank you for all the feedback shared so far!

Whether it's reports about deployment issues with `pg_tde`, integration with KMS, missing features or gaps in our documentation, we truly appreciate it! Your input helps us build a better, more complete solution and to properly prioritize what's next.

https://percona.community/blog/2025/05/08/progress-report-on-pg_tde-ga-extension-is-nearer-every-day/

Lesson learned during work on TDE:

Users don’t understand security



PostgreSQL already has data in transit encryption: **TLS/SSL**

https://www.postgresql.org/docs/current/ssl-tcp.html

NO, pg_crypto is **not TDE**

Try it out!

Percona PostgreSQL GitHub Repo

Nightly builds repo

PERCONA

for PostgreSQL

Thanks for attention and hope to see you encrypted!