PERCONA

pg_tde

Transparent Data Encryption in an extension

(plus a bit...)

Who is telling this story?

- Alastair Turner
  - Technical Evangelist at Percona
- Reformed presales techie
- Database things since the 90s
- Postgres things since 2002
  - Including making Drupal work better with Postgres circa 2010

The exam question

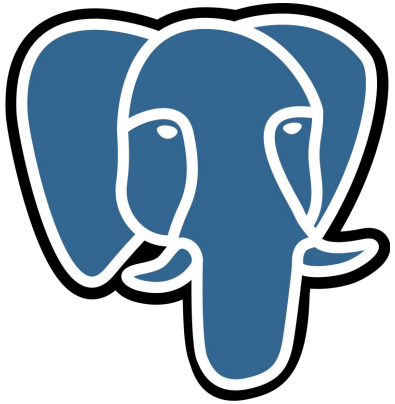
- Why did you create the extension in the first place?
- What do you wish past you would have known about being an extension maintainer?
- If your library ever got a big overhaul, why was that?
- How do you find co-conspirators for your work?
- Where do you see the project going?
- What contributions would you love to see?

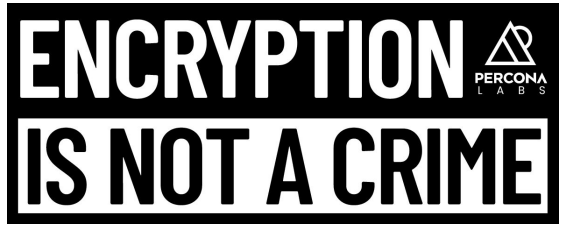
We'll answer…

- Why did you create the extension in the first place?
  - Why TDE?
- What do you wish past you would have known about being an extension maintainer?
- If your library ever got a big overhaul, why was that?
  - There's one in progress, see What's Next?
- How do you find co-conspirators for your work?
  - *This, mainly :)*
- Where do you see the project going?
  - What's next?
- What contributions would you love to see?
  - How can you get involved?

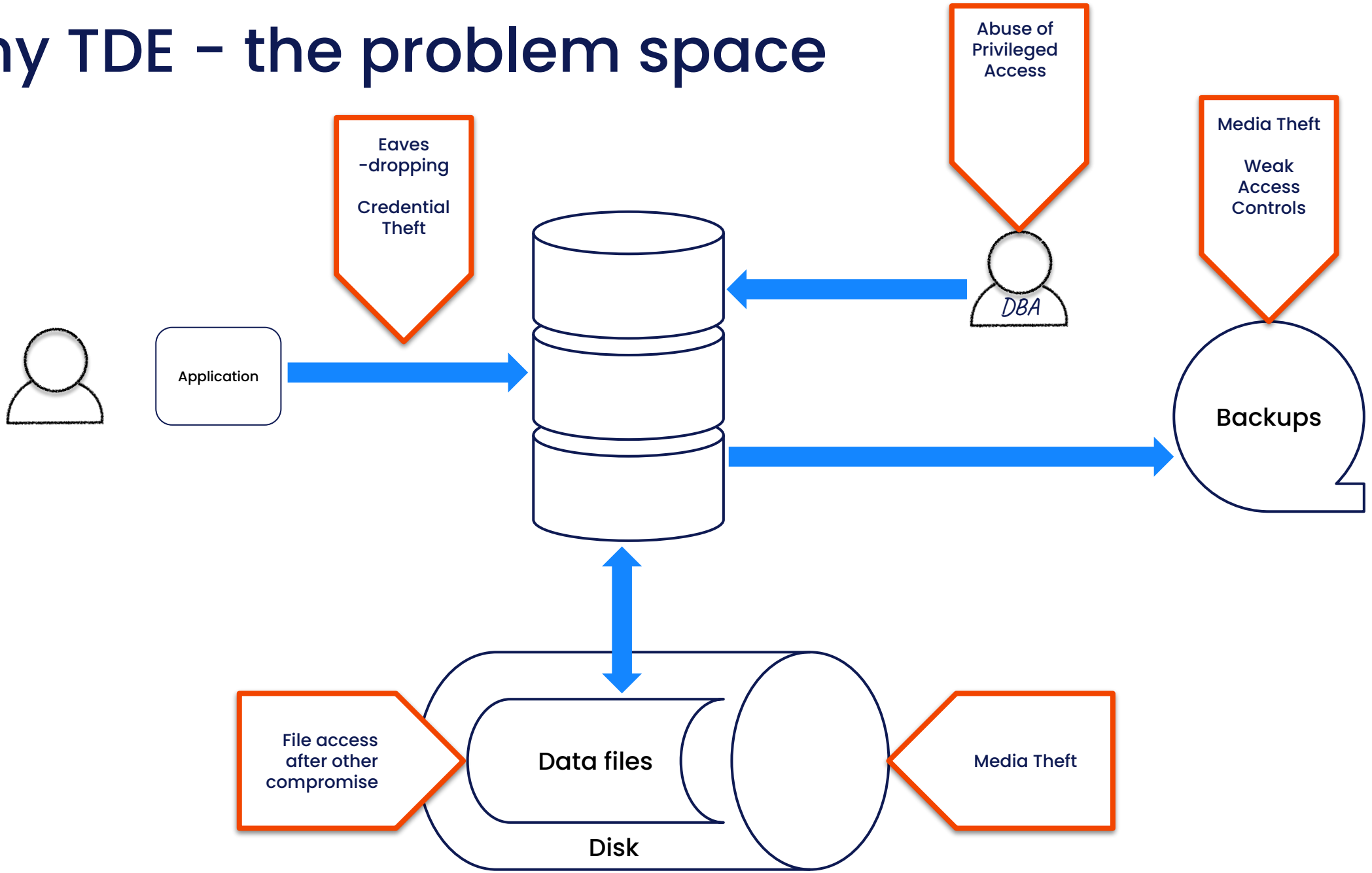
Agenda

- Who is telling this story?
- Why TDE?
- What have we built?
- What's next?
- How can you get involved?

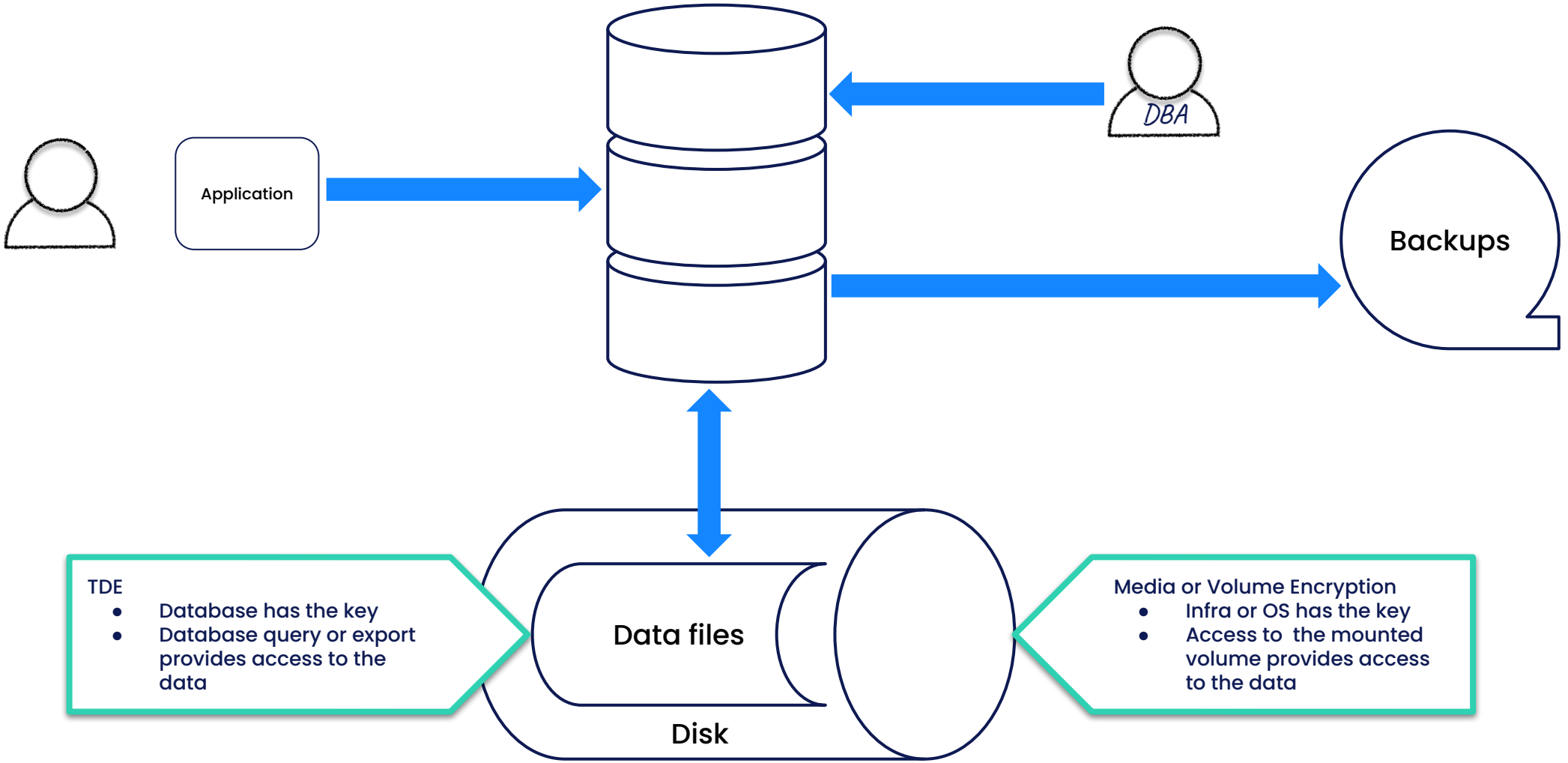




Why TDE - the problem space



Why TDE - the solution space



Why TDE in an extension

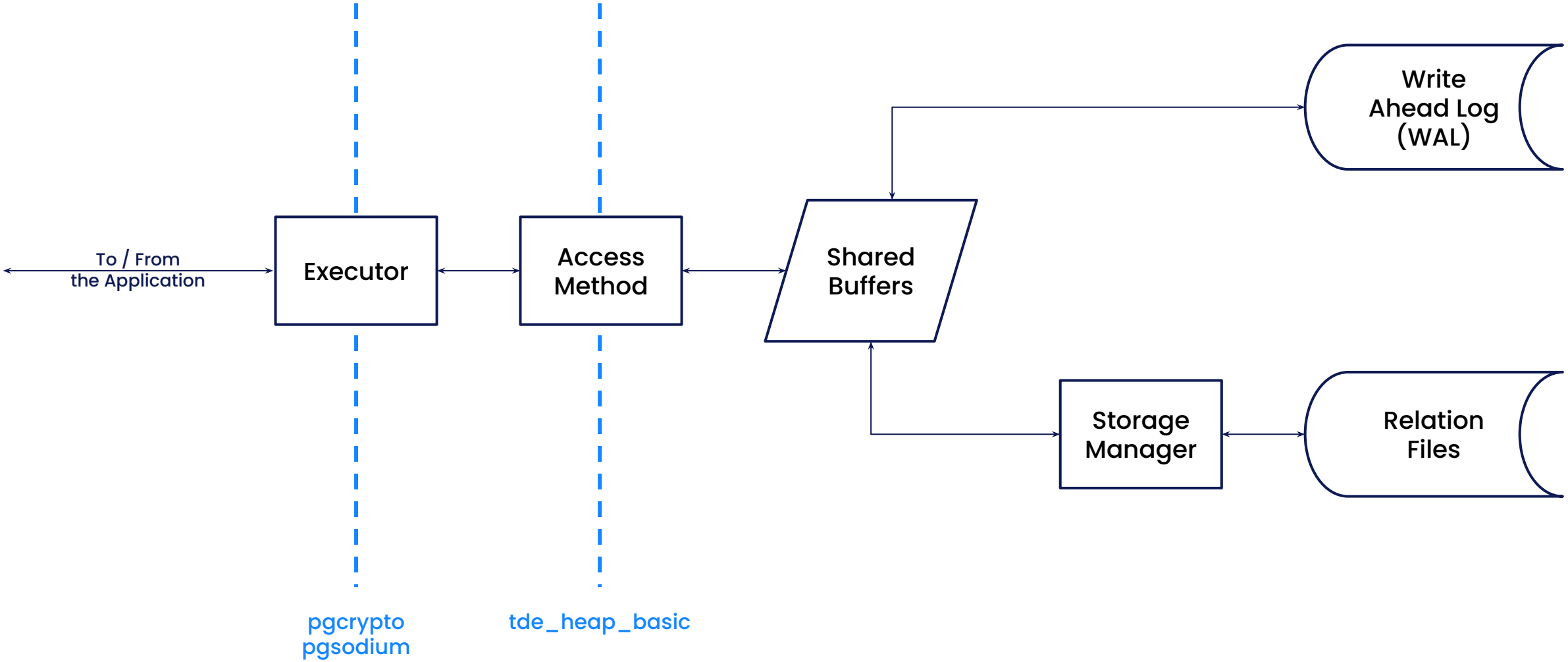
- Multiple efforts to include TDE on core Postgres have stalled
  - First in 2016
  - Big, intrusive, hard to digest patchsets
  - Lots of disagreement around key management
- Cryptography extensions don’t provide encryption transparently
- Keep the impact on those not using TDE to a minimum

Why pick TDE to work on?

- Domain experience in TDE at Percona
  - Percona Distribution for MySQL and MongoDB

- Explore the options for extensibility and faster turnarounds in the Postgres world

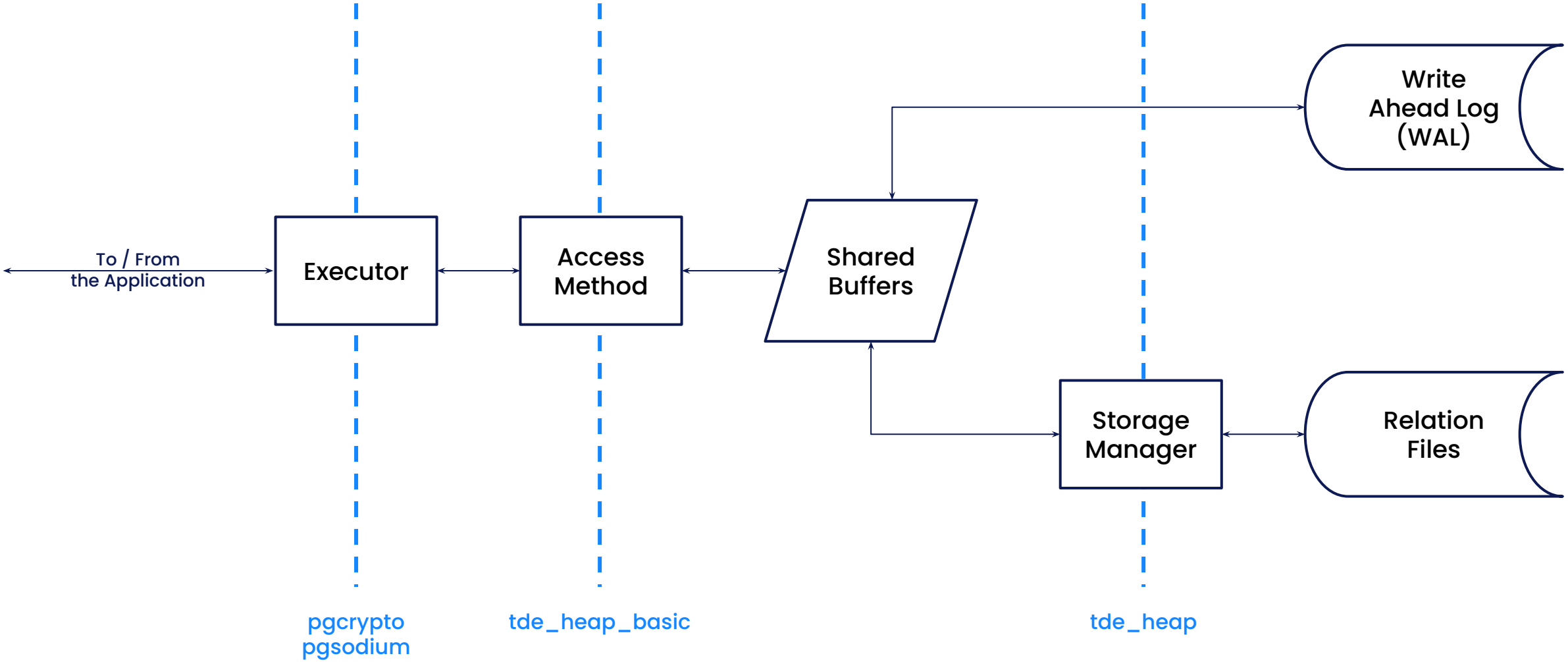
What have we built?



How far did it get us?

- TDE in an extension
- Can only encrypt table content
- Currently in public beta
- Encrypt/decrypt individual tuples
- For tuples that have externally stored columns(toast), the external values are encrypted/decrypted separately
- Write-Ahead Log (WAL) data for tables created using the extension
- Temporary tables created during the database operation for data tables created using the extension

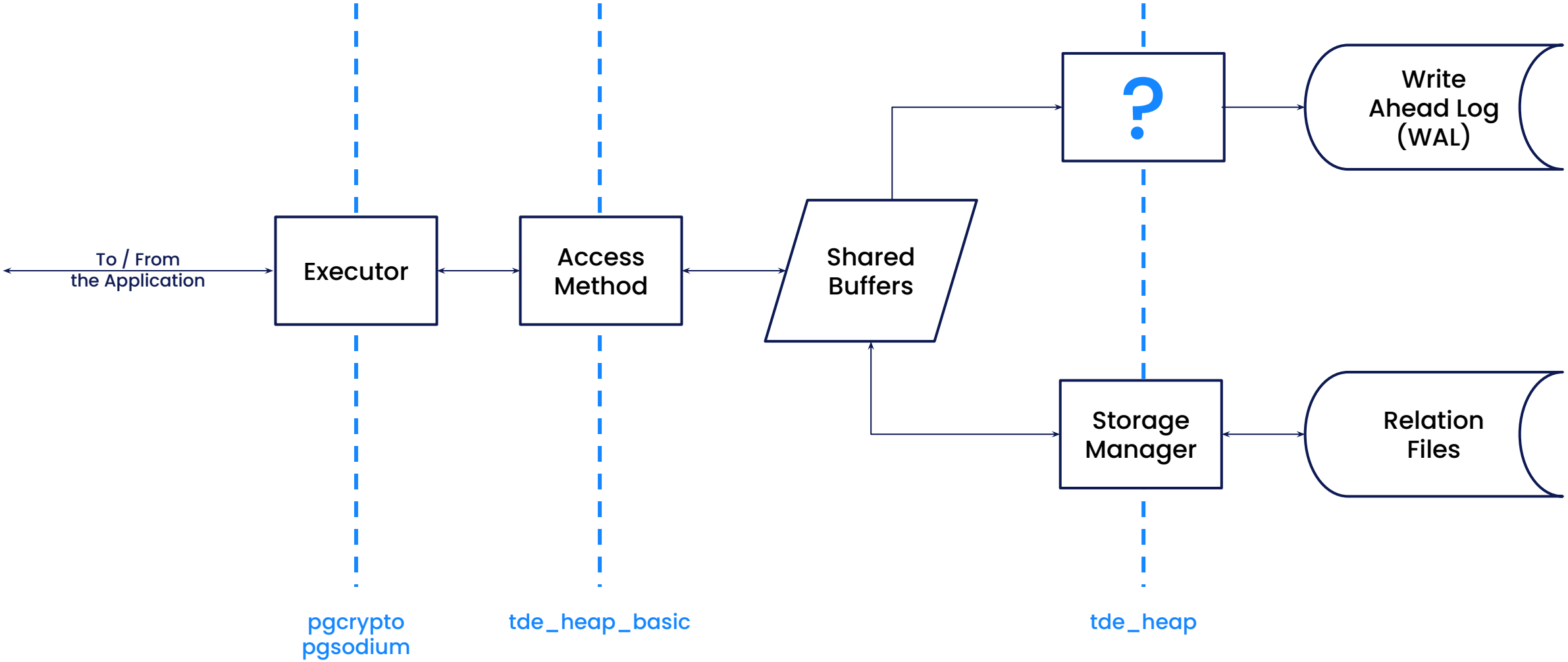
What's next?



How far will that get us?

- TDE for tables and indexes on encrypted tables
- Requires a bit more extensibility than is currently exposed
  - Starting from an SMGR patch proposed by Neon
- Encrypt/decrypt on block level.
- Tech preview shipping in November

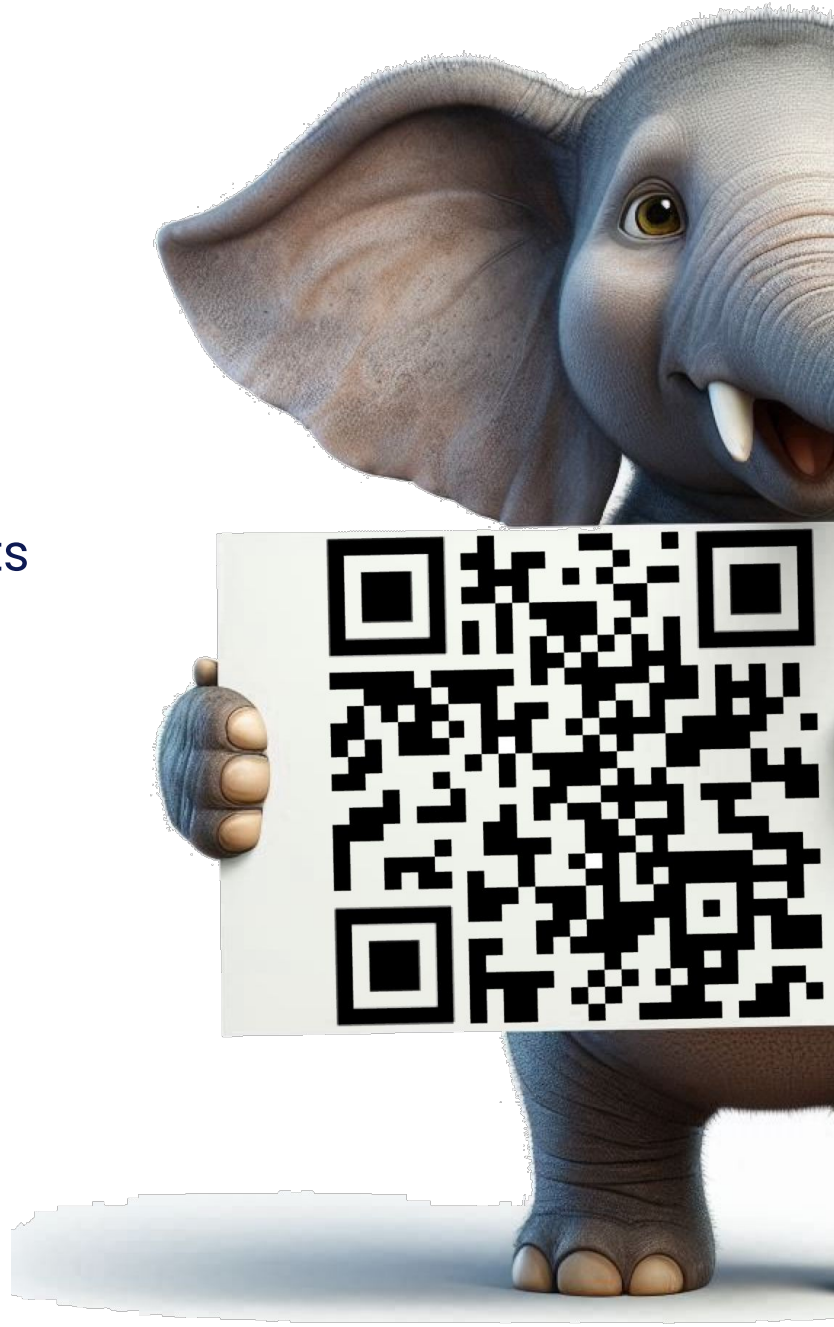
And another goal...



How can you get involved?

- Get current Beta of the extension and try it out
- Give us some feedback

- If you have an interest in the additional extension points we're proposing, get in touch
  alastair.turner@percona.com
  jan.wieremjewicz@percona.com
  - Would these changes be useful to you?
  - Are we just doing it all wrong?
  - .....



https://github.com/percona/pg_tde

Thank You!