CYBERTEC PostgreSQL Enterprise Edition - PGEE

PGEE Security @ CYBERTEC

Date: 2024-08-28
Publisher: CYBERTEC Security team

Table of contents

PGEE: Comprehensive database security

CYBERTEC PostgreSQL Enterprise Edition (PGEE) is a CYBERTEC product which has been designed for enterprise-grade security in critical environments that require additional **security** as well as regular auditing. This solution focus heavily on **compliance** and **business critical** workloads for various industries, including but not limited to:

- Banking and financial services
- Governments and defense
- Critical national infrastructure
- Business-critical missions

Ensuring security is key and therefore our first priority is to provide customers with **encryption at every level** while providing cutting edge performance.

PGEE offers comprehensive database security and provides the necessary tooling to enable enterprise success, focusing on these key aspects:

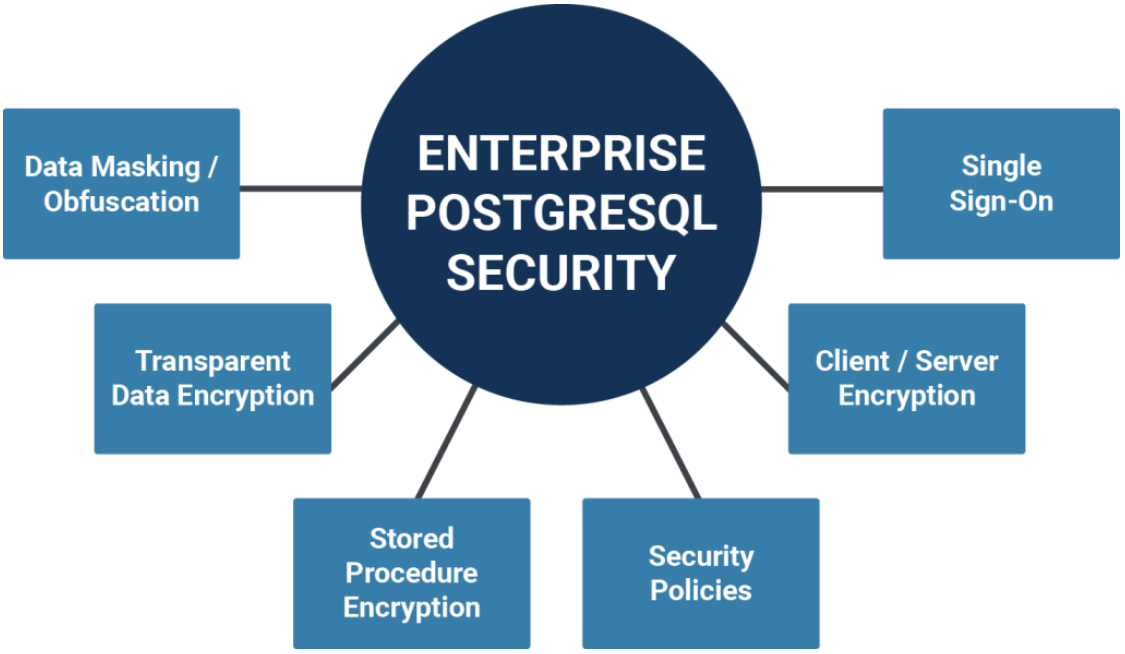
- Encryption at every level
- Secure software development
- Auditing and certification

This document describes how PGEE achieves those goals running your enterprise workload.

PGEE: Encryption at every level

Ensuring industry-standard encryption at every level is key to success. PGEE provides exactly that. We ensure safety at **all levels**:

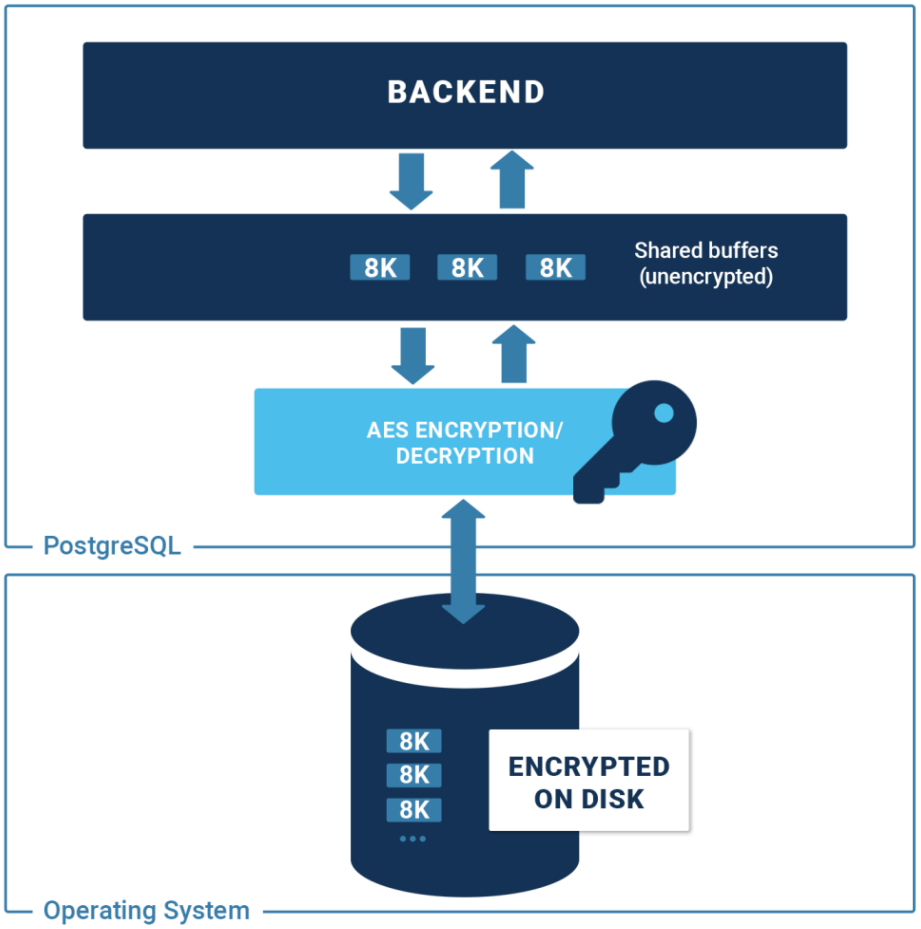
- **Encryption on disk** through "Transparent Data Encryption"
- Secure **key management**
- **Client / server** encryption
- Secure and transparent replication
- Encryption of **stored procedures**
- **Data Masking** and data exchange



All those features come with auditing as well as rapid security updates.

TDE: Transparent Data Encryption

"Transparent Data Encryption" (TDE) is one of the key features of PGEE. It automatically encrypts data on disk and ensures safe storage in every possible way.



PGEE uses **hardware acceleration** to quickly encrypt data sent to disk and quickly decrypt data during reads, providing maximum protection, allowing for **maximum transparency** on the application side. No application changes are required to use a TDE-encrypted database.

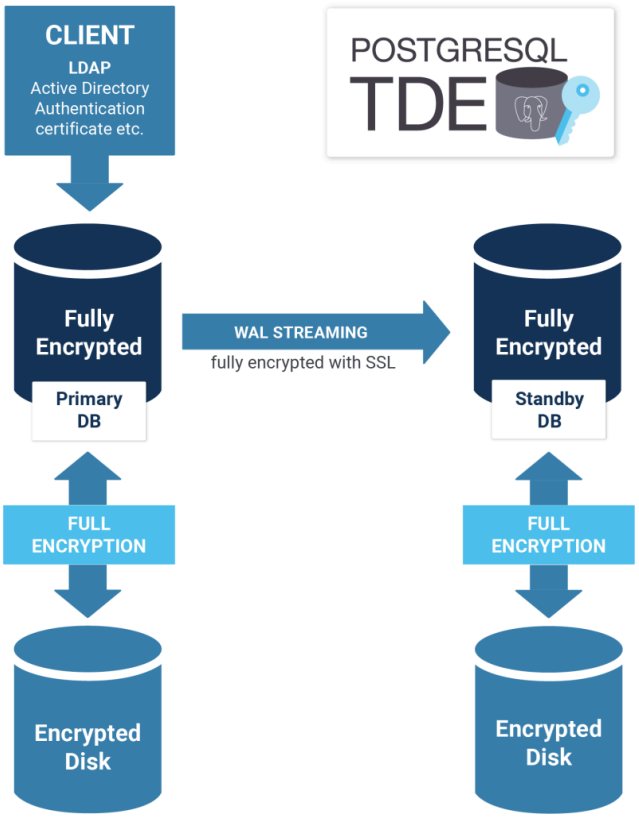
We use industry-standard encryption algorithms for maximum security and portability across platforms and environments. Easy integration is therefore ensured.

Integration into existing infrastructure

PGEE can easily be integrated into existing infrastructure. We ship PGEE in various ways:

- RPM / DEB packages (RHEL and derivatives, SLES, Debian, Ubuntu)
  - ready-to-use "drop-in replacement" for PostgreSQL
- Docker / Podman containers
- Ready-to-use Kubernetes / OpenShift operators
- Easy to use Windows installers
- **Optional:** Automatically available through CYBERTEC Scalefield

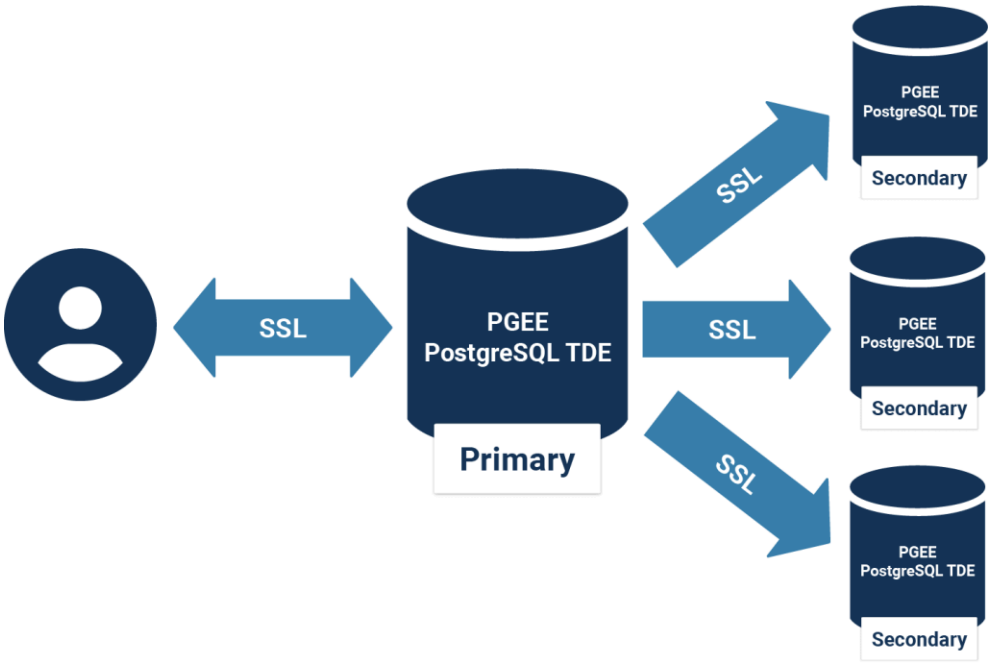
All our solutions are fully **High Availability ready** and are fault-tolerant by design.



PGEE integrates easily into existing **key management software** through an extensible and easy to use **plugin infrastructure**. Key management software such as **KeyCloak and many others** can easily be connected to PGEE.

Enterprise-grade High Availability

Business-critical applications are exactly that: critical to the business. There is no such thing as “downtime”. PGEE is ready for High Availability (HA) and clustering out of the box. Even in a HA cluster, all components are safely encrypted at every level.



Replicas as well as the communication between servers are secure by default. PGEE allows for many important features such as:

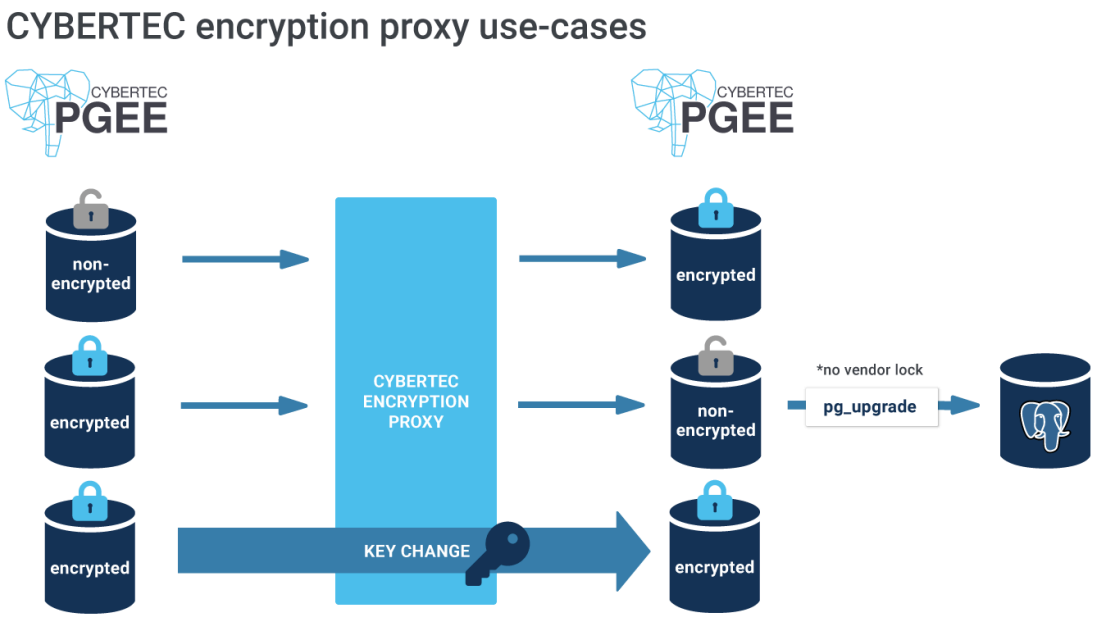
- Automatic failover
- Transparent clustering
- Easy scalability

We secure every part of the way, while eliminating the workload imposed on database administrators and infrastructure teams.

Managing PGEE efficiently

Avoiding vendor lock-in is important to us. We prefer for our **customers to be free** and able to make their own choices for their infrastructure. As part of PGEE we therefore provide mechanisms to freely move from standard PostgreSQL to PGEE and back.

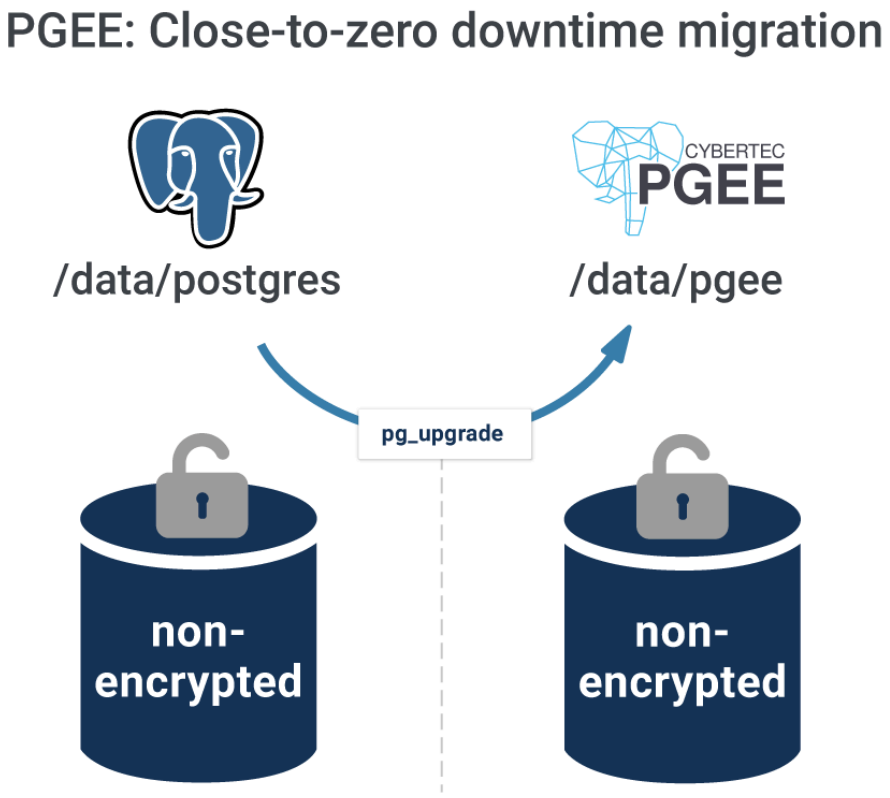
Our encryption proxy allows you to make those transitions easily and quickly.



Various options are available and are permanently supported by PGEE – even across versions and major releases.

Moving from PostgreSQL to PGEE

Moving to PGEE is as simple as deploying standard PostgreSQL. Simply install our software and run simple scripts to switch between PostgreSQL and PGEE.

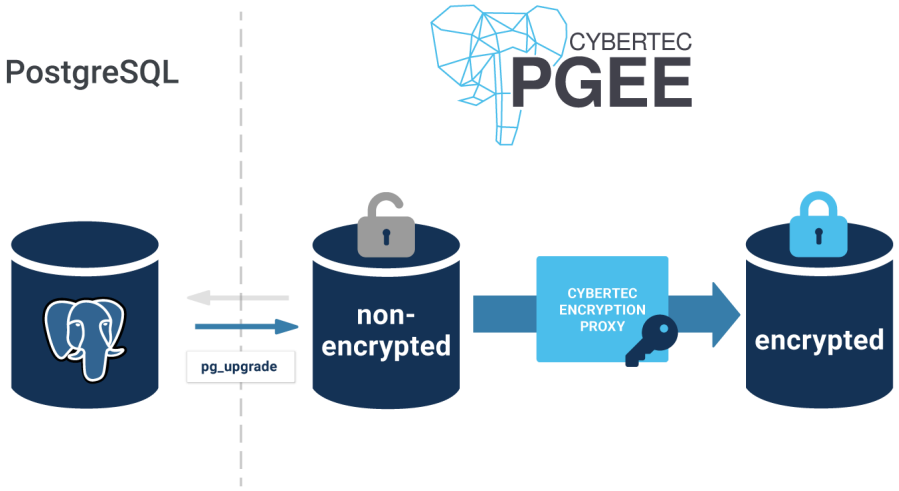


Enterprise grade features:

- **Close-to-zero downtime** migration
- **Non-destructive** migration
- Works for **every version** of PGEE

Deploying encrypted PGEE

Simply use an existing database instance and replicate it into a fully encrypted environment quickly with zero risk. During and after the transition, your original database will stay operational which ensures safety, compliance as well as fault tolerance.



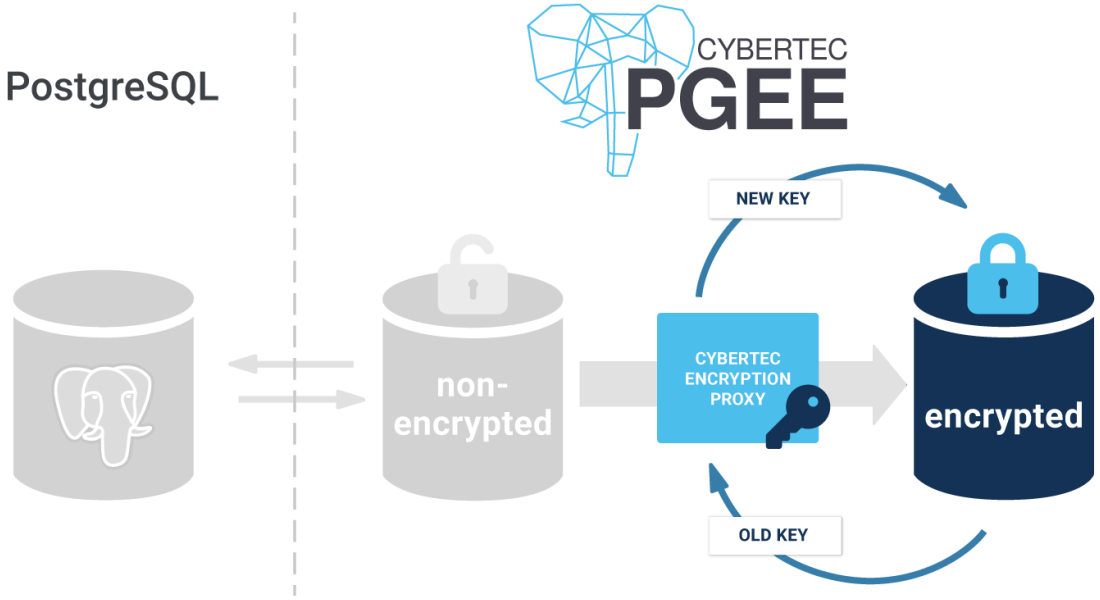
Enterprise-grade features:

- **Close-to-zero downtime** migration
- Create **multiple encrypted systems** concurrently
- **End-to-end encryption** at all time
- **Full compliance** with current security standards
- **Non-destructive** migration
- Integrates with all commonly used KMS software
- Works for **every version** of PGEE

Changing encryption keys

Meeting compliance requirements and safety standards is important. Therefore we allow users to quickly change encryption keys at any point in time.

Our PGEE encryption proxy allows you to do just that:

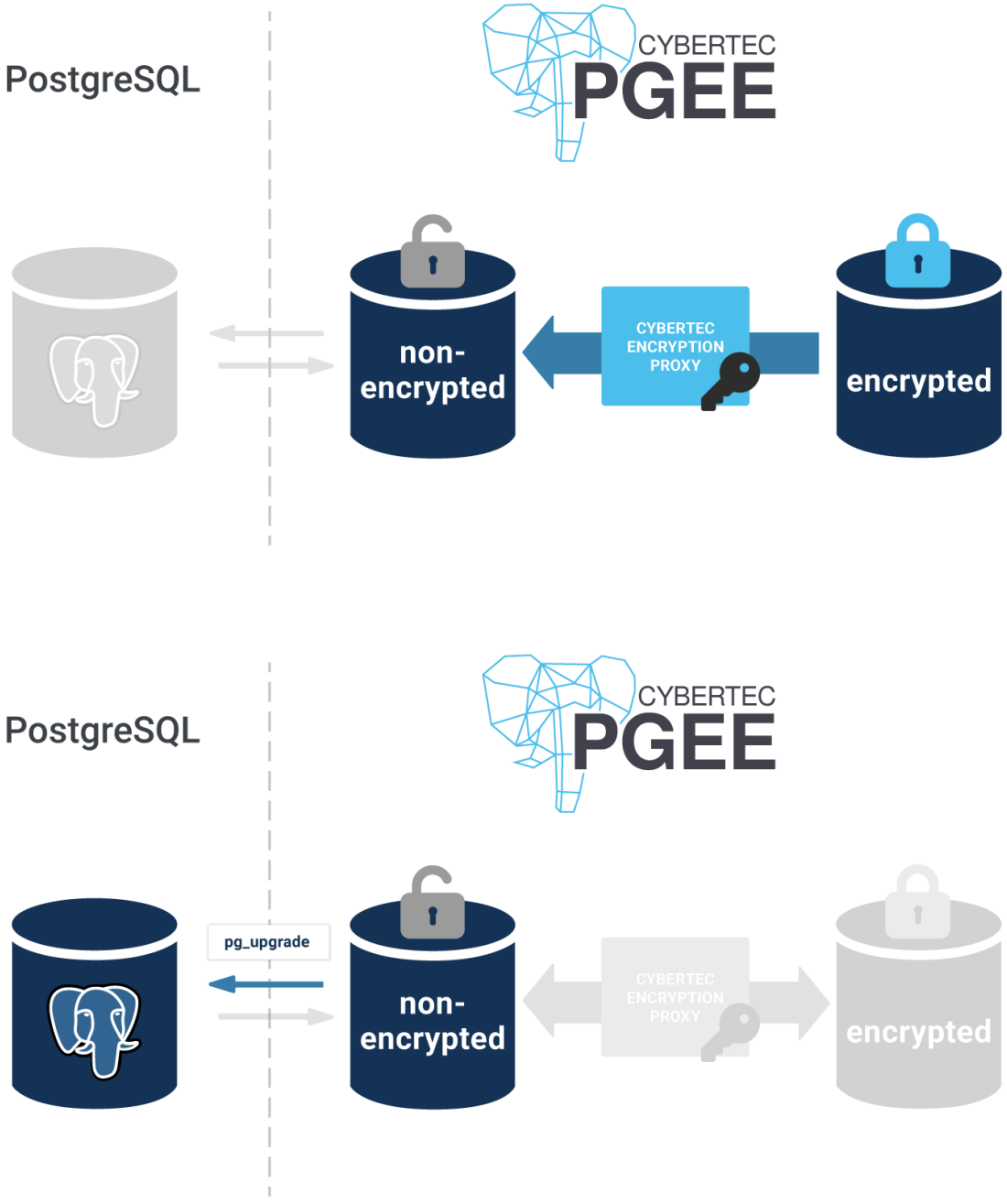


Enterprise grade features:

- **Close-to-zero downtime** key changes
- **End-to-end encryption** at all time
- **Full compliance** with current security standards
- **Non-destructive** key changes
- Works for **every version** of PGEE

PostgreSQL ←→ PGEE: Moving between the worlds easily

Customers can decide whether to use encryption or not. We thus allow to easily encrypt database instances and provide an easy transition between full PGEE encryption, non-encrypted PGEE and standard PostgreSQL:



Users can decide at any point how to **encrypt or decrypt data** and how to store data in the most secure way while maintaining **compliance** and **security** standards.

CYBERTEC: Secure software development

We at CYBERTEC believe in secure software development. Our development model is based on core principles which focus heavily on security and compliance:

- Automated **software validation**
- Fully automated **security checks**
- Regularly performing **CVE checks** and alerting

We immediately notify our customers and inform them about security updates and risks to ensure maximum security, compliance and help maintaining data security at any point. In times of ransomware and constant security attacks on critical systems it is important to stay at the forefront of security to protect customers and data.

We always keep in mind that data is not just data: we might store somebody's passport, the cash in your bank account, or private medical data which can save a life.

"Security is not to be discussed – it has to be taken seriously."

With this mindset we help secure data around the world powering critical infrastructure.

Building software safely

We follow a professional approach which is aware of security at any point. Our process ensures that all software shipped by CYBERTEC has undergone comprehensive manual, as well as automated testing, conforming to the strictest of all standards:

All packages are constantly checked, rechecked and updated as new threats emerge.

Managing security and CVEs

The secret sauce is a full integration of openly available security related information and our software development process. All **repositories are inspected** by automated processes to **detect flaws** in libraries, components and processes. Automated end-to-end **testing and auditing** allows us to eliminate threats and security leaks quickly, while staying in constant touch with the customer.

Security and end-customer experience

What does this mean for our customers? It means…

- **Security** at **all times**
- Speedy **security updates**
- Automated **alerting**
- Fully **awareness** of existing threats
- Total visibility and **transparency**
- "Next level" **compliance**

We can ensure the speedy delivery of critical security updates as well as background information which helps to…

- Classify operation risks
- Cooperate with auditors
- Meet security standards
- Manage updates and operations

Our team encourages customers to report security related issues in a cooperative and constructive manner.

CYBERTEC certifications

CYBERTEC is audited on a regular basis. We comply with legislation around the world (GDPR, CCPA, Popi Act, etc.)

CYBERTEC is ISO certified, showing our long term commitment to compliance and security.

PGEE: Additional security features

PGEE has many more security related features which are easy to use and apply in real life. Some of the key features are:

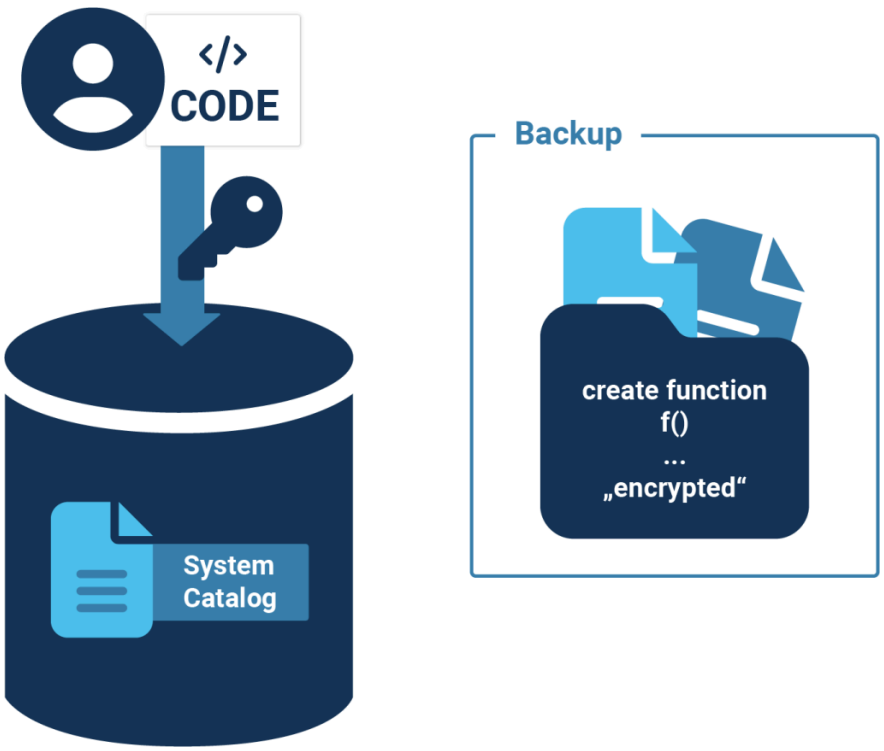
- Encrypted server side stored procedures
- Data masking and obfuscation
- Extended database auditing
- Password security checks
- Rule-based maintenance permissions
- Integrated security auditing

In this section the key aspects of this functionality are explored.

Encrypted stored procedures

Many companies rely on "Intellectual Property" (IP). Protecting valuable knowledge is therefore key to the success of a company or an organization.

PGEE offers the ability to encrypt stored procedure code to hide valuable business secrets from curious eyes.



Simply mark your procedures as encrypted. PGEE will automatically take care of the rest, allowing you to do what you can do best – operate and scale your business. No need to work – your code is safe.

Data masking and obfuscation

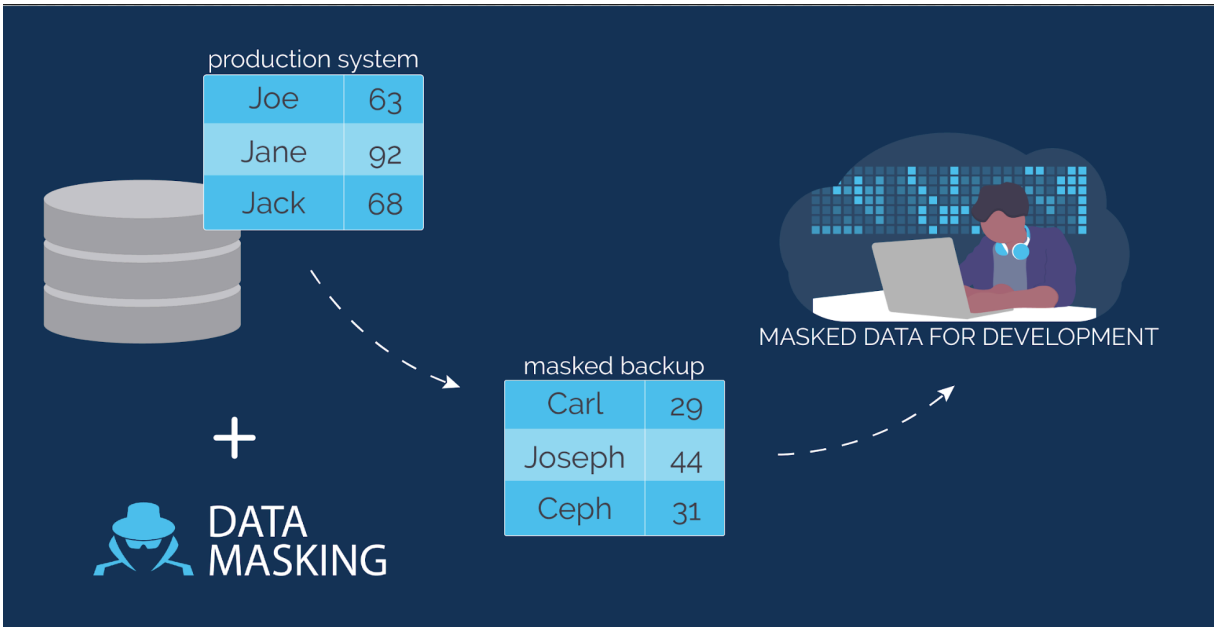
Data protection and privacy laws put severe restrictions on which data can be seen by whom. PGEE supports those efforts and provides end users with "Data Masking and obfuscation".

Simply define rules and apply them on your data. It will allow you to easily **produce secure real-life data sets** which can be used for…

- Software development
- Quality management
- Data analysis

…without providing users with access to **critical confidential information**.

Here is how it works:



Keep your data safe while providing a solid test infrastructure for your software development team.

Extended database auditing

Database auditing is an essential practice in today's data-driven world. With the increasing importance of data security and compliance, organizations must ensure that their databases are properly monitored and controlled to prevent unauthorized access, changes, or exfiltration.

How does **PGEE help with auditing**?

- **Full audit** trail of all important database events
- Audit trails as SEPARATE UNIX user
  - **Prevent user from changing their own audit trail**
  - Full security **separation**

PGEE auditing is optimized for high-performance while maintaining easy usability.

Password security checks

PGEE tracks failed database login attempts, such as due to password mismatch, and automatically locks accounts to prevent brute-force attacks.

User passwords are checked for strength based on configurable rules, and reusing old passwords can be prohibited.

Rule based maintenance permissions

Changing the data structure in your database can be dangerous. In the case changes are deployed while the database is in production, problems might happen.

“Dedicated permissions for maintenance windows”

PGEE allows you to associate permissions with maintenance windows. You can prevent changes to your data structure during certain periods while allowing them during a maintenance window. PGEE therefore greatly reduces the risk of accidentally modifying applications while they are operational.

Integrated security auditing

In PGEE we do more than provide **cutting-edge security** -- we also make it easier to **enforce** those **policies** and ease the burden of administration. At CYBERTEC, we are aware that security problems are often not related to a lack of tooling but to a lack of oversight and visibility.

The enterprise capabilities of PGEE allow you to:

- **See all permissions** immediately
- Define **declarative** permissions system
- Automatically calculate the difference between the desired and real state
- **Fix** permissions **automatically**

In PGEE permissions audits are a core component of the system which allows you to

- Meet **compliance** requirements
- Gain deeper understanding
- **Prevent security breaches**
- **Automate security** improvements

Security audits are an integral part of PGEE, which greatly reduces the workload on administrators while mitigating risk.

FAQ: Frequently asked questions

This section will handle frequently asked questions and helps you get started quickly:

Question:
Where does PGEE store the encryption key?

Answer:
PGEE provides a plugin infrastructure which allows you to store the key anywhere. However, we strongly recommend to NOT store the key on the same server but instead use a professional KMS (Key Management System) to handle keys

Question:
In case of encryption: Does the application see real or encrypted data?

Answer:
The application can see data normally which is why we call the feature "transparent" data encryption. Encryption happens behind the scenes and therefore does not affect your application. Your applications will work normally.

Question:
Can I start a PostgreSQL instance with PGEE?

Answer:
No, you have to run a simple pg_upgrade process to PGEE first. However, this can be done in only a few seconds and this upgrade will not destroy your old database installation.

Question:
May I run more than just one version of PGEE concurrently on the same server?

Answer:
Of course. There are no restrictions. We operate just like PostgreSQL.