
SECURE OPEN SOURCE SOFTWARE (OSS)
Data protection, access controls, and a hardened, secure Postgres that protects against all known vulnerabilities, so you can build with confidence.
EDB

Data protection, access controls, and a hardened, secure Postgres that protects against all known vulnerabilities, so you can build with confidence.

THE CHALLENGES

Postgres® has become famous among many developers as Stack Overflow's favorite database. Today's developers and database administrators prefer open source solutions like PostgreSQL over legacy databases because of its cost-effectiveness, customization, active community support, rapid innovation, and adherence to SQL standards. But while PostgreSQL provides many benefits, it also introduces a challenge in identifying and mitigating potential security vulnerabilities in open source software deployments. Enterprises must ensure their applications use hardened versions of PostgreSQL that have gone through extensive testing, comply with industry certifications, and reduce the risk of malware attacks. Enterprises must also ensure that customer data is protected and access to databases is controlled.

- **Managing OSS vulnerability:** Identifying and mitigating potential security vulnerabilities in Postgres deployments is a critical and demanding task. Organizations need to prioritize using trusted and vetted sources for open source components to reduce the risk of introducing vulnerabilities or exploits into their deployments.
- **Protecting customer data:** Securing customer data is paramount. Encrypting data at rest and in transit is essential to protect against unauthorized access and data breaches, as the attack surface extends to the database itself, the infrastructure it runs on, and the applications that interact with it.
- **Enforcing Zero Trust Access:** Large organizations face challenges in controlling database access due to multiple teams seeking to use customer data for analytics and AI products.

THE SOLUTION

EDB Postgres AI is a trusted enterprise provider for hardened Postgres software packages, protecting against all known vulnerabilities and enabling you to operate confidently with open source. Also, additional enterprise security features protect customer data and limit database access providing additional layers of security.

- **Hardened Postgres:** Obtain a secured Postgres distribution that goes through secure design principles in coding practices, comprehensive testing, verification, and other activities to minimize vulnerabilities.
- **Trust Center:** Get access to EDB's responses to enterprise-grade security concerns and an overview of EDB's commitment to embedding data privacy and security in every part of the business.
- **Enterprise-grade security:** Protect your application and customer data with transparent data encryption (TDE), SQL protection, audit trails, and data redaction. Control access with role-based access control (RBAC) and fine-grained data access control down to specific rows.
- **Software bill of materials (SBOM):** Gain visibility with EDB's SBOM, which offers a detailed inventory of components and dependencies that comprise a software package, including up-to-date license reporting.

KEY RESOURCES

- **Related Products and Solutions**
  - EDB Postgres AI »
  - EDB Postgres Advanced Server »
  - Enterprise-Grade Postgres »
- **Blogs and Content**
  - How to Secure PostgreSQL: Security Hardening Best Practices & Tips »
  - EnterpriseDB Raises the Bar for Postgres Security and Compliance with Transparent Data Encryption »
  - Elevating Postgres Security with the EDB Trust Center »
  - Security Best Practices for Postgres 2023 Update »
  - Trust Center »
  - AI Data Security with Postgres: Best Practices and Compliance »
  - Documentation for Security Features »
  - EDB CVE Assessments »
- **Webinars and Demos**
  - EPAS15 - The Most Secure Postgres »
  - Best Practices in Security with PostgreSQL »

EDB

THE BENEFITS

Enjoy rapid value delivery with automated security safeguards. Code, deploy, and release new software with hardened Postgres and other enterprise security features to develop confidently, ensure customer trust, and keep customer data secure.

- **Build secure applications:** Develop secure applications with EDB as a trusted Postgres provider that follows National Institute of Standards and Technology (NIST)'s Secure Software Development framework. Get over 50 signed repositories covering 10 various Postgres extensions used by over 1,500 companies.
- **Customer trust:** Increase trust in your company's care of customer data. Adhere to local compliance rules to expand the user base and increase retention.
- **Secured data:** Reduce risk of vulnerabilities and eliminate the effort required to build a secure data environment. Operate confidently, knowing that 100% of the EDB code base is hardened and backed by enterprise-grade security best practices.
- **Compliance adherence:** Keep up with compliance requirements, even with industry-specific regulations such as PCI-DSS, HIPPA, or other government Zero Trust framework requirements.
- **Transparency and visibility into your software supply chain:** EDB's SBOM reports help track changes in Postgres deployments, making it easier to identify and mitigate potential security vulnerabilities.

THE OUTCOMES

- Program with confidence, knowing that your version of Postgres has gone through extensive testing and verification.
- Protect customer data with additional safety and security measures, providing peace of mind for both the organization and its end-users.
- Prevent unauthorized access to databases and customer data.
- Maintain a log of all activity to help adhere to compliance standards.

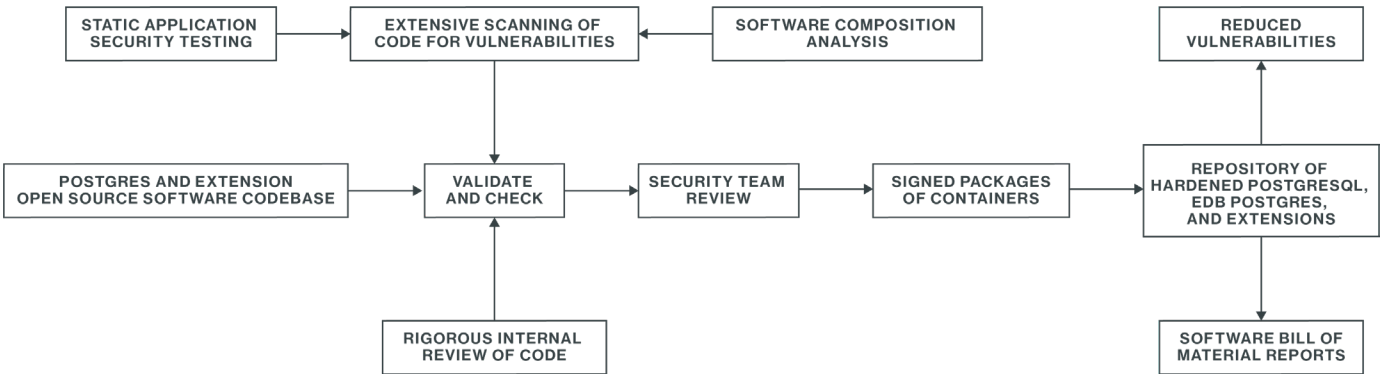

Figure 1. EDB Postgres AI secures your open source software so you can operate with confidence and compliance. 100% of the EDB codebase undergoes secure design principles in coding practices, comprehensive testing, verification, and other activities to minimize vulnerabilities.

FREQUENTLY ASKED QUESTIONS

Q: What do we mean by "hardened Postgres"?
A: Hardened Postgres refers to EDB reviewing Postgres and related extensions, building and signing packages, and hosting in our own repo to ensure that SLAs can be met for bug fixes and security updates. We ensure that 100% of the codebase undergoes secure design principles in coding practices, comprehensive testing, verification, and other activities to minimize vulnerabilities. Then, we patch the vulnerabilities and undertake other preventive measures to ensure that the repositories are safe against any vulnerabilities. The checked repository is then built into a signed package, which gives enterprises peace of mind.

Q: How does EDB provide data protection and access controls?
A: Here's how EDB can help:

- Data protection: Customers can protect their data with TDE, data redaction, and using a hardened version of Postgres.
- Access Controls: EDB provides RBAC and fine-grained data access down to specific rows.

Q: What is TDE?
A: Transparent data encryption (TDE) encrypts any user data stored in the database system. This encryption is transparent to the user. User data includes the actual data stored in tables and other objects as well as system catalog data such as the names of objects.

Q: What do we mean by audit logging?
A: Audit logging refers to allowing database and security administrators, auditors, and operators to track and analyze database activities. EDB audit logging generates audit log files, which can be configured to record information such as:

- When a role establishes a connection to an EDB Postgres database
- The database object role creates, modifies, or deletes when connected to EDB
- When any failed authentication attempts occur

Q: What is meant by data redaction?

A: Data redaction limits sensitive data exposure by dynamically changing data as it is displayed for certain users. For example, a social security number (SSN) is stored as 021-23-9567. Privileged users can see the full SSN, while other users see only the last four digits: xxx-xx-9567.

Q: How does EDB help protect against SQL injection attacks?
A: EDB does two things:

- Provides a layer of security in addition to the normal database security policies by examining incoming queries for common SQL injection profiles.
- Gives the control back to the database administrator by alerting the administrator to potentially dangerous queries and by blocking these queries.

Q: Where can someone go to read about EDB's compliance and gain more information about EDB's approach to security?
A: Customers and others can go to the EDB Trust Center, which provides at-a-glance visibility into EDB's security posture. The Trust Center enables easy navigation into public documents that attest to EDB's security policies, compliance certifications, and other relevant documents, streamlining security reviews from customers, partners, and prospects alike.

Q: What is an SBOM?
A: Software bill of materials (SBOM) reports offer a detailed inventory of components and dependencies that comprise a software package, enabling you to more easily identify and mitigate potential security vulnerabilities.

Q: How does someone get access to SBOM reports?
A: The SBOM reports will be available for software customers who are entitled to them in the EDB Repos browsing page once they have logged in with their enterprisedb.com account.