EDB SQL/Protect

PostgreSQL databases, have long been known to be the most secure open source databases!

SQL/Protect adds another powerful layer of security inside the data center and under the control of DBAs.

SQL/Protect Highlights

DBA-Managed SQL Injection Protection

» Preventing attacks is normally the responsibility of each application developer, but with SQL/Protect, DBAs can now provide a standardized layer of protection.

Protection Against Multiple Attack Types:

» Unauthorized Relations

» DDL Commands

» SQL Tautology

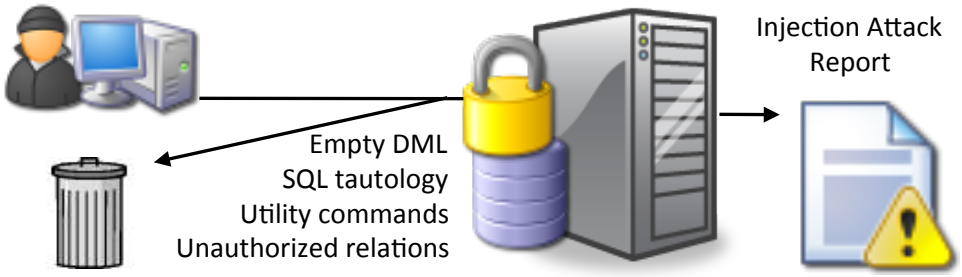
» Unbounded DML

Role-Based Flexibility

» You can have protected and non-protected roles each covering a whole class of individual users. Each role can be customized for the type of injection attacks that are monitored and rejected.

Better Protection for Your Critical Data

Modern businesses want to take full advantage of open source databases and the benefits they offer, but are worried that they can't deliver the type of security features that the more expensive proprietary databases do. Given the rash of high-profile SQL injection attacks that have occurred lately this is a reasonable concern.
IT organizations can rest assured that SQL/Protect delivers security on par with any modern database when used with Postgres Plus security features like ANSI SQL GRANT and REVOKE, external authentication using LDAP, PAM or Kerberos, Group/Role support, granular object permissions, built-in security auditing, and server code obfuscation.



Protection Against Four Different Attacks

In addition to setting normal table restrictions, DBAs can have SQL/Protect learn your application's data access patterns and enforce them to **prevent access to unauthorized relations**.
Secondly, SQL/Protect can **block utility DDL command** execution, which are rarely needed by users during standard processing.
The most frequent technique used in SQL injection attacks is issuing a WHERE clause condition that is always true. SQL/Protect **blocks queries that use a tautological conditional clause.**
Finally, when it comes to the most dangerous attack type, SQL/Protect **prevents unbounded DML statements** (UPDATE and DELETE statements with no WHERE clause) that can corrupt or delete your data.

Easy Installation and Management

SQL/Protect is pre-installed as part of Postgres Plus Advanced Server and installs in minutes for community PostgreSQL. It installs directly into the database server close to your data and under centralized control. Everything is controlled and monitored by the DBA through simple database commands. In minutes you can configure roles to protect, covering whole classes of users and have SQL/Protect start learning 'friendly' activities in your applications.

Stop SQL Injection Attacks with SQL/Protect

Add SQL/Protect to existing security:

- ANSI standard GRANT and REVOKE on all tables, sequences and functions
- View Security Barriers
- Row Level Security (Postgres Plus Advanced Server)
- Server side procedural language obfuscation
- External Authentication: LDAP, PAM, Kerberos, SSPI, RADIUS
- Group and Role support
- SSL Encrypted Sessions
- Granular object permissions
- Large object access controls

Contact us today about:

- Software Subscriptions
- Technical Support 24 x 7 x 365
- Migration Assessments
- Training (Online / On-Demand)
- Professional Services

Call the nearest location below or Email: sales@enterprisedb.com

www.enterprisedb.com

EnterpriseDB Locations

Netherlands
The Netherlands/EMEA +31 70 361 1774

India
Pune +91-20-30589500/01

United States
Bedford, MA +1 781-357-3390

Japan
Tokyo +81-50-5532-7038

Three Levels of Protection

SQL/Protect does more than just shield you from destructive or compromising attacks. Its intelligent and assists you in your deployment of better protection.
In **Learn mode** SQL/Protect tracks the activities of protected roles and records the relations used by the roles, and records them for future use. This relieves DBAs from specifying lots of rules and lets you run your application and let SQL/Protect learn its 'normal' safe usage characteristics.

In **Passive mode**, SQL/Protect issues warnings if protected roles are breaking the defined rules, but does not stop any SQL statements from executing. This is an excellent configuration for testing your defenses before deploying them to your production system.
Finally, in **Active mode**, SQL/Protect not only prevents attacks but logs attack activity for later analysis.

```
edb=> CREATE TABLE appuser_tab (f1 INTEGER);
NOTICE:  SQLPROTECT: This command type is illegal
                                    for this user
CREATE TABLE
edb=> DELETE FROM appuser_tab;
NOTICE:  SQLPROTECT: Learned relation: 16666
NOTICE:  SQLPROTECT: Illegal Query: empty DML
DELETE 0
```

DBA-Managed SQL Injection Protection

The usual methods of protecting against SQL injection attacks rely on laborious, careful, and consistent programming techniques by one or more programmers in each application written against the database. With SQL/Protect, a DBA has a consistent centralized and standardized security layer inside the database. Protection is thus easier to manage and monitor and is consistent regardless of how many applications or programmers are accessing your data.

Attack Data for Analysis

Once a Role is running in active mode, SQL/Protect keeps track of each attempt of an attack. This allows you to review and analyze the frequency and type of attacks your database may be subjected to as well which user or class of users are the source of the attacks. You can also write your own custom reports against the collected data using normal SQL commands.

EnterpriseDB and Postgres Plus are trademarks of EnterpriseDB Corporation. Other names may be trademarks of their respective owners. Copyright © 2014. All rights reserved. 20140905