The dvdrental database follows several built-in and configurable security practices that contribute to protecting the data and controlling access.

1. Role-Based Access Control (RBAC)

* PostgreSQL uses roles (users and groups) to manage access.
* The database has a superuser (postgres) and other users can be created with limited privileges.
* Permissions are granted explicitly using GRANT statements, ensuring least-privilege access.

2. Authentication Mechanisms

* PostgreSQL uses the pg\_hba.conf file to define how users are authenticated.
* Common methods used include:
  + md5 (hashed passwords)
  + scram-sha-256 (more secure, if configured)
* This ensures that unauthorized users cannot access the database.

3. Privilege Control on Database Objects

* Access to tables, views, schemas, and other objects is controlled via:
  + GRANT SELECT, INSERT, UPDATE, etc.
  + REVOKE to remove access
* Users only have permissions that are explicitly assigned, protecting sensitive data like customer information or payment history.

4. Schema Usage Restrictions

* The public schema is restricted using GRANT USAGE and GRANT CREATE commands, preventing unauthorized users from creating or accessing objects in it.

5. Encrypted Connections (Optional)

* PostgreSQL supports SSL/TLS connections (ssl = on in postgresql.conf), which encrypts traffic between the client and server.
* If enabled, this prevents eavesdropping on credentials and queries over the network.

6. Logging and Auditing

* PostgreSQL logs connections, disconnections, queries, and authentication failures if configured:
  + Parameters like log\_connections, log\_disconnections, log\_statement are available.
  + This helps track access history and detect suspicious activity.

7. Backups and Recovery

* Regular backups are assumed to be in place using tools like pg\_dump.
* These backups should be securely stored and access-restricted to ensure data integrity and availability.

8. Row-Level Security (Optional/Configurable)

* PostgreSQL supports Row-Level Security (RLS) to limit which rows a user can access based on policies.
* If configured, it ensures that users can only access data they are authorized to see.