

Comment Casement maintient les données de chaque entreprise séparées.

Le problème des bases de données partagées

Casement utilise une base de données partagée, multi-locataires : les biens, baux et locataires de chaque entreprise vivent dans les mêmes tables. C'est efficace à exploiter, mais cela signifie qu'un seul bug dans le code applicatif -- un filtre oublié, une requête copiée-collée -- pourrait en théorie exposer les données d'une entreprise à une autre. Casement est conçu pour que cette erreur ne puisse pas se produire, même si elle est commise.

Ce qui est réellement appliqué

- **Sécurité au niveau des lignes**

Postgres impose l'isolation des locataires au niveau du moteur de base de données, sur chaque table de locataire -- pas comme une logique applicative qu'un futur bug pourrait contourner.

- **Double sécurité**

Chaque requête liée à un locataire filtre aussi explicitement par ID d'entreprise dans le code applicatif, en plus de la politique au niveau de la base de données -- deux couches indépendantes, pas une seule.

- **Un rôle d'exécution restreint**

L'application se connecte à Postgres avec un rôle délibérément à faibles privilèges (`pms_app`), distinct du rôle élevé utilisé uniquement pour les migrations.

- **Authentification par entreprise**

Chaque requête est authentifiée par un JWT contenant l'entreprise de l'utilisateur, vérifié sur chaque route protégée.

Voir la démo en direct : demo.casement.eu

Demander une démo : casement.eu

Ce document décrit l'architecture actuelle d'isolation des données de Casement, telle qu'implémentée aujourd'hui. Il ne s'agit pas d'un audit de sécurité tiers finalisé ni d'une certification de conformité.