

Toad® for Oracle - Sensitive Data Protection

Trouvez et contrôlez les données sensibles dans l'ensemble de vos bases de données Oracle de façon rapide et simple.

Les violations de données sont plus fréquentes que jamais et concernent des entreprises de toute taille. Cette tendance inquiète de nombreuses entreprises sur les conséquences d'une violation de données : impact financier, réputation entachée, perte d'activité éventuelle. En tant qu'administrateur de bases de données Oracle, vous êtes responsable de la protection des données contenues dans vos bases de données. C'est un rôle qui peut s'avérer complexe alors même que vous gérez une multitude d'applications et de bases de données réparties dans le Cloud et dans l'ensemble de l'entreprise. Vous en avez assez de parcourir manuellement des milliers de tables dans plusieurs bases de données pour localiser les données sensibles au moyen des noms de colonnes ?

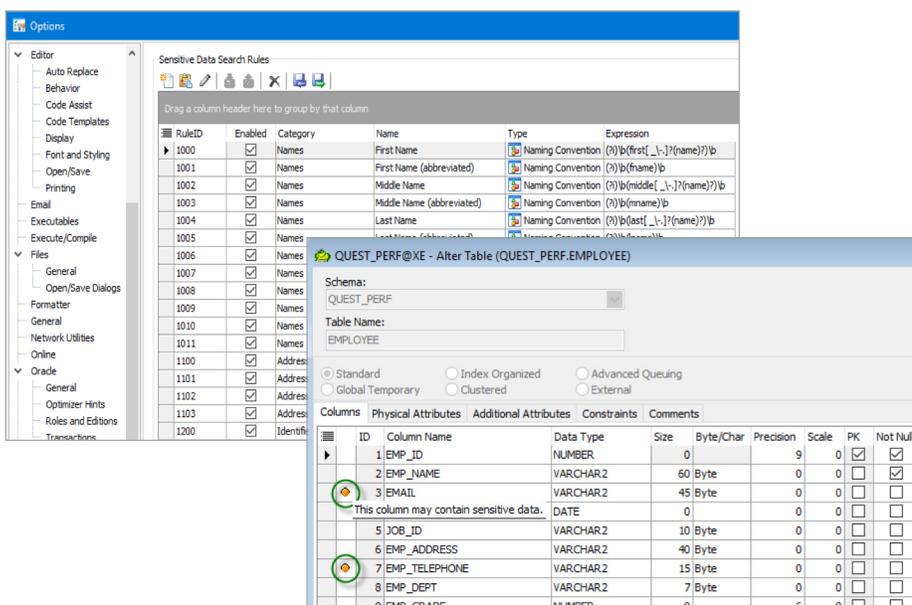
Lorsque vous avez recours aux outils d'un fournisseur qui s'appuie sur les métadonnées pour identifier les données sensibles, la localisation de ces données sur l'ensemble de vos bases de données peut prendre un temps considérable. Ces outils peuvent être inefficaces et ignorer l'existence de certaines données sensibles, car ils supposent que les tables et colonnes de vos bases de données suivent des conventions de nommage strictes. Et si vous pouviez utiliser une technologie et une automatisation de recherche sophistiquées pour rationaliser ce processus ? Vous gagneriez du temps et réduiriez les risques.

Avec la solution Toad® for Oracle - Sensitive Data Protection, vous pouvez effectuer une recherche avec un outil

Simplifiez et automatisez l'identification de données sensibles et la création de rapports. Appliquez ensuite rapidement les mesures de protection des données nécessaires.

AVANTAGES :

- Identifiez plus rapidement les données sensibles sur l'ensemble de vos bases de données Oracle
- Notifiez les développeurs automatiquement lorsque des champs de données sensibles sont référencés lors de la création de code
- Automatisez le processus de détection et simplifiez la création de rapports
- S'intègre avec de nombreuses fonctionnalités Toad, telles que Editor, VOE et DB Health Check



Appliquez vos règles de recherche pour identifier les données sensibles dans l'ensemble de vos bases de données Oracle.

CONFIGURATION SYSTÈME REQUISE

Comme pour Toad for Oracle Professional Edition ou les versions ultérieures. Toutefois, un accès à Internet est requis pour activer la licence pour le module Sensitive Data Protection.

qui procède à un échantillonnage des données dans l'ensemble de vos tables, à l'aide de règles prédéfinies contenant des expressions régulières pour identifier les données sensibles. Cette solution vous permet de personnaliser et de créer vos propres règles et de redéfinir vos paramètres de recherche sur l'ensemble des bases de données Oracle. Ensuite, après avoir localisé vos données sensibles dans une table, vous pouvez appliquer les techniques de rédaction, de chiffrement et d'audit natives d'Oracle.

Les conséquences de non-conformité avec la réglementation sur la confidentialité des données (par exemple le RGPD et le Data Privacy Act de Californie) peuvent être considérables, inclure des amendes lourdes et ternir la réputation de votre marque. Préparez-vous. Réduisez votre risque d'exposition et assurez la conformité en localisant les données sensibles dans vos bases de données Oracle et en appliquant la protection adéquate de façon simple et rapide.

FONCTIONNALITÉS

Sensitive Data Awareness

Disponible dans Toad for Oracle Professional Edition 13.1 et les versions ultérieures.

- **Règles personnalisables** : propose des règles configurables pour identifier vos données sensibles.
- **Sensitive Data Awareness** : signale automatiquement l'utilisation de données sensibles dans les éditeurs d'objets et de code.

Sensitive Data Search

Uniquement disponible dans le module Sensitive Data Protection, qui fait partie de Toad for Oracle Professional Edition 13.2 (et les versions ultérieures). Remarque : Une clé de licence distincte est nécessaire pour activer Sensitive Data Protection.

- **Règles personnalisables** : propose des règles configurables pour définir ce que vous considérez comme des données sensibles dans les schémas de colonnes et de données.
- **Sensitive Data Search** : effectue des recherches parmi les schémas de base de données Oracle en interrogeant les métadonnées et les données.
- **Sensitive Data Protection** : vous permet d'appliquer les mesures de protection adéquates à l'aide des fonctionnalités Oracle de chiffrement, de rédaction et d'audit des données.
- **Workflow rationalisé** : permet aux administrateurs de bases de données et aux délégués à la protection des données d'appliquer des mesures de protection in situ.
- **Création de rapports** : exécutez des rapports sur une ou plusieurs bases de données. Exporte les résultats dans le cadre du respect de la confidentialité des données sensibles.
- **Automatisation** : automatise les fonctions de recherche et de création de rapports pour identifier et localiser les données sur lesquelles aucune stratégie n'a encore été appliquée.
- **Database Health Check** : vous permet d'inclure et d'automatiser la protection des données sensibles avec d'autres tâches courantes d'administration de bases de données.

PROFIL DE QUEST

Quest fournit des solutions logicielles adaptées au monde de l'informatique d'entreprise en rapide évolution. Nous simplifions les défis associés à l'explosion des données, à l'expansion dans le Cloud, aux datacenters hybrides, aux menaces de sécurité et aux exigences de conformité. Notre gamme de solutions couvre la gestion des bases de données, la protection des données, la gestion unifiée des terminaux, la gestion des accès et des identités, ainsi que la gestion des plateformes Microsoft.