

# ORACLE DATABASE VAULT

## PRINCIPAUX AVANTAGES

### ORACLE® 11g DATABASE

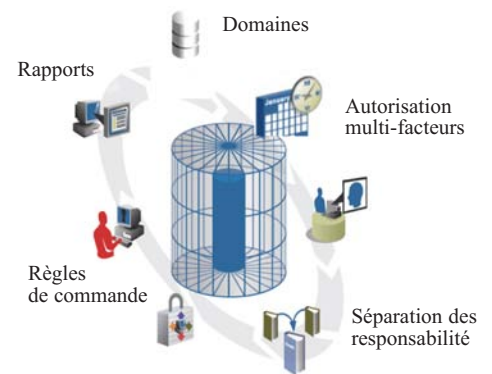
- Interdit l'accès aux données applicatives sensibles pour les utilisateurs disposant de privilèges élevés
- Contrôle l'accès aux applications, aux bases de données et aux données avec des options de sécurité d'une grande souplesse
- Implémente la séparation des responsabilités
- Disponible pour Oracle Database 10g Version 2, Oracle Database 9i Version 2 et Oracle Database 11g Version 1
- Certifié pour les applications Oracle PeopleSoft



*Oracle Database Vault fournit des contrôles internes stricts pour assurer la conformité réglementaire et la protection contre les risques internes. Oracle Database Vault empêche non seulement les utilisateurs disposant de privilèges élevés de visualiser les données applicatives sensibles, mais il assure aussi la mise en œuvre des règles définissant par qui, quand, où et comment les applications, les bases de données et les données peuvent être accédées. Oracle Database Vault protège de façon transparente les applications de base de données sans nécessiter la moindre modification des applications existantes.*

## ORACLE DATABASE VAULT

Les réglementations telles que la loi Sarbanes-Oxley (SOX), le standard de sécurité de données PCI (*Payment Card Industry*), ou encore la loi de portabilité et de responsabilité de l'industrie de la santé (HIPAA – *Healthcare Insurance Portability and Accountability Act*) imposent des contrôles internes stricts pour protéger des informations sensibles telles que les données financières, les dossiers médicaux et les références de cartes de crédit contre tout accès ou modification non autorisés. Oracle Database Vault constitue une solution de sécurité puissante et facile à utiliser avec la base de données Oracle, permettant aux entreprises de respecter facilement les réglementations actuelles ou futures au sein de leurs applications existantes ou nouvelles. Les risques internes constituent une préoccupation croissante pour les entreprises du monde entier. L'étude CSI/FBI 2005 portant sur la sécurité et la criminalité informatiques a montré que plus de 70% des pertes de données et des attaques informatiques ont été effectuées de l'intérieur, c'est-à-dire par des personnes disposant au moins d'un certain niveau d'accès au système et à ses données.



Présentation d'Oracle Database Vault

Pour respecter les réglementations et se protéger contre les risques internes, deux évolutions importantes doivent être apportées aux environnements existants :

- des contrôles bloquants pour restreindre les accès non autorisés aux données sensibles par les utilisateurs disposant de hauts privilèges ;
- des contrôles souples et adaptables pour définir par qui, quand, où et comment les applications, les bases de données et les données peuvent être accédées.

Les Domaines, Règles et Facteurs d'Oracle Database Vault (décrits ci-dessous) travaillent ensemble au sein de la base de données pour restreindre l'accès, même pour les utilisateurs les super-utilisateurs, sans interférer avec l'administration

## ORACLE DATABASE VAULT

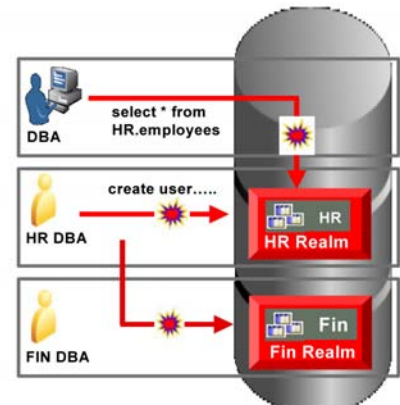
### PRODUITS DE SÉCURITÉ ASSOCIÉS :

- Oracle Audit Vault
  - Regroupe de façon transparente les données d'audit de plusieurs bases de données
  - Simplifie le reporting de conformité réglementaire grâce à des rapports prédéfinis
  - Détecte les risques très en amont avec des alertes
  - Gère les règles d'audit pour toutes les bases de données
  - Capable de monter en puissance grâce à la technologie robuste de la base de donnée Oracle
  - Permet de créer des rapports spécifiques en s'appuyant sur un datawarehouse ouvert
- Oracle Advanced Security
  - Chiffrement transparent des données sans modification du code SQL applicatif
  - Supporte AES 256
  - Authentification stricte
  - Chiffrement réseau
- Oracle Label Security
  - Contrôle d'accès basé sur des étiquettes
  - Sécurité multi-niveaux
  - Protège les données sensibles
  - Intégré avec Oracle Database Vault grâce à des facteurs d'étiquettes
  - Critère Commun d'Evaluation pour EAL4
- Oracle Secure Backup
  - Chiffrement de la base de données et du système de fichiers pendant les sauvegardes sur bande
  - Intégré avec l'utilitaire Oracle Recovery Manager (RMAN) et supporte jusqu'à 256 bits AES

quotidienne de la base de données. Ces fonctionnalités peuvent être utilisées de façon souple et adaptable pour appliquer les règles de sécurité, sans avoir à modifier les applications existantes.

### CONTRÔLE DES UTILISATEURS À HAUTS PRIVILÈGES

Les administrateurs informatiques, les administrateurs de bases de données et les administrateurs d'applications occupent des postes de confiance au sein d'une entreprise. Mais la conformité réglementaire, l'externalisation, le regroupement des applications et la prise en compte croissante des risques internes ont entraîné une quasi-obligation de contrôler très strictement l'accès aux données applicatives sensibles. La modification a posteriori du code applicatif existant avec de nouveaux contrôles d'accès peut s'avérer à la fois longue et coûteuse, voire inenvisageable pour beaucoup d'entreprises. Avec les domaines (*Realms*) d'Oracle Database Vault, les entreprises peuvent empêcher les utilisateurs à hauts privilèges, y compris les DBA, d'accéder aux données applicatives. Les domaines sont simples à définir et peuvent être placés autour d'une application complète ou d'un ensemble de tables aussi rapidement que facilement.



*Domaines, Règles et Facteurs d'Oracle Database Vault*

### SOUPLE ET ADAPTABLE

Les Règles et Facteurs d'Oracle Database Vault sécurisent étroitement les applications en limitant par qui, quand, où et comment les bases de données, les données et les applications peuvent être accédées. Plusieurs facteurs tels que l'adresse IP et la méthode d'authentification peuvent être utilisés de façon souple et adaptable pour appliquer les contraintes d'autorisation, sans avoir à modifier les applications existantes. Par exemple, l'accès à la base de données peut être restreint à un serveur précis du niveau médian de l'architecture. Des règles liées aux commandes SQL peuvent être définies afin d'offrir un contrôle encore plus fin.

### SÉPARATION DES RESPONSABILITÉS

Oracle Database Vault assure une séparation des responsabilités et protège la base de données contre les modifications non autorisées. Oracle Database Vault définit en standard trois responsabilités distinctes pour l'administration de la sécurité, la gestion des comptes et la gestion des ressources. Par exemple, Oracle Database Vault empêche un DBA disposant du privilège de création d'utilisateurs de créer un nouvel utilisateur si ce DBA ne dispose pas de la responsabilité adéquate. Vous pouvez déclinier la responsabilité d'administration des ressources en 3 responsabilités distinctes : les responsabilités de sauvegarde, de performance et d'application des correctifs. Vous avez également la possibilité de regrouper des responsabilités.

### VALIDATION DES APPLICATIONS

Oracle a certifié Oracle Database Vault pour les applications PeopleSoft. Des scripts de configuration faciles à utiliser et des instructions étape par étape peuvent être téléchargés sur le réseau OTN (*Oracle Technology Network*). Les validations d'Oracle E-Business Suite et de Siebel sont actuellement en cours et devraient être achevées dans le courant de cette année.

### POUR NOUS CONTACTER

Pour en savoir plus sur Oracle, consultez le site [oracle.com](http://oracle.com) ou appelez le +1.800.ORACLE1 pour contacter un représentant Oracle.