



**<Insert Picture Here>**

## **Технологии защиты от инсайдеров для центров обработки и хранилищ данных**

Дмитрий Шепелявый, MBA, PMP, CISSP  
Директор по продуктам безопасности, Oracle СНГ

# План презентации

- Вопросы к безопасности информации в хранилище
- Обзор решений Oracle по защите данных в хранилищах
- Database Vault
- Audit Vault

# Вопросы к безопасности в СУБД

- Имеет ли ваш администратор СУБД фактический доступ к конфиденциальной информации? SQL запрос
- Уверены ли вы, что сотрудники имеют доступ только к необходимой им информации?
- Знаете ли вы, когда, и к какой информации пользователь имел доступ?
- Уверены ли вы, что обнаруживаете все попытки несанкционированного доступа к информации в БД? Приложение
- Уверены ли вы, что информация на физических носителях и в резервных копиях надежно защищена от утечки? Удаленный WEB доступ
- А ваши базы данных продаются на Горбушке?

# “KEY to the KINGDOM”

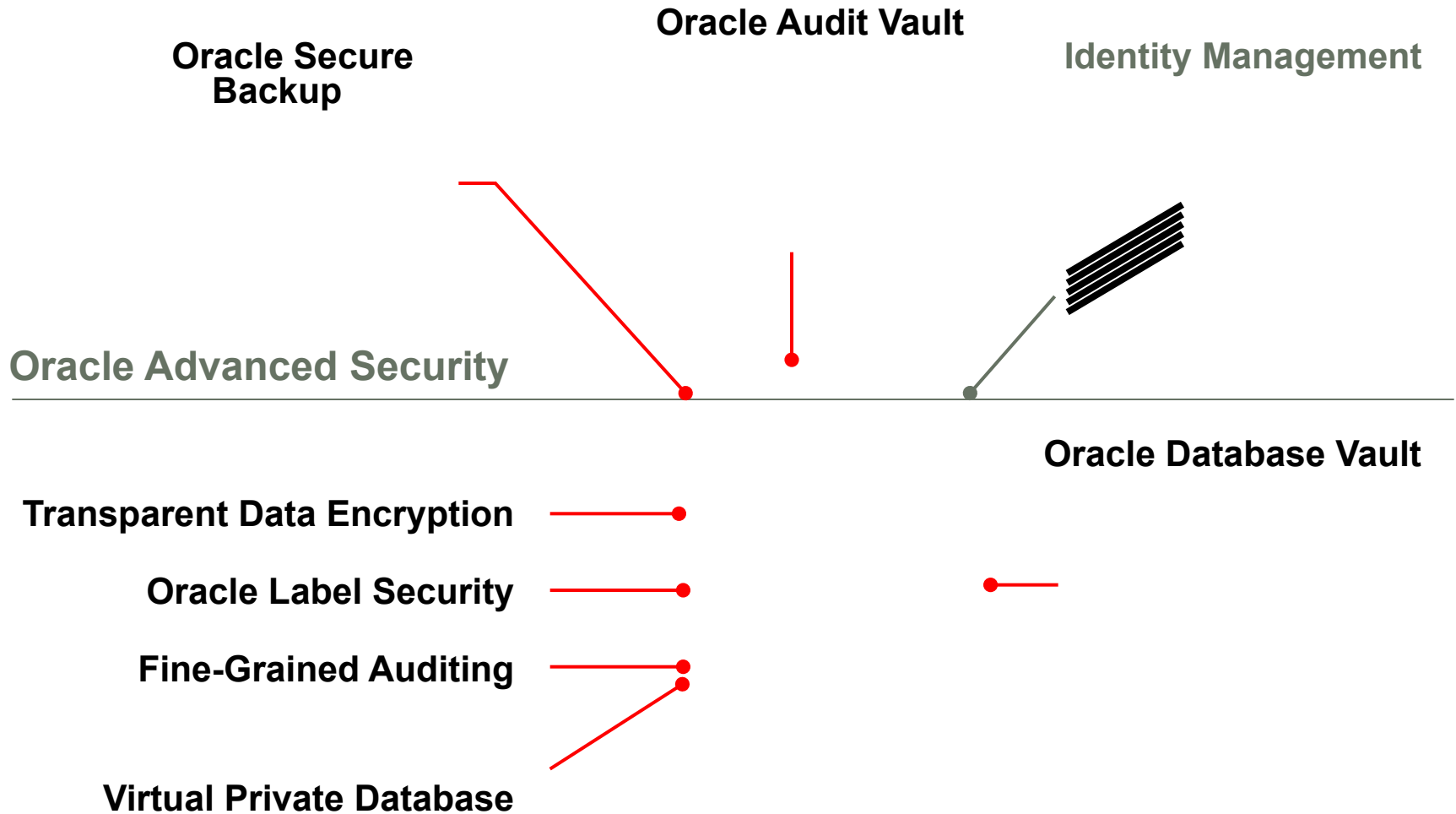
Connect / as SYSDBA

These crimes were all  
thieves **inside**

В Нью-Йорке завершился суд по делу  
о краже клиентской базы из  
Morgan Stanley.

В утечке оказался виноват инсайдер.  
Суд приговорил его к 26 годам лишения  
свободы и \$850K штрафа

# Базовые средства безопасности

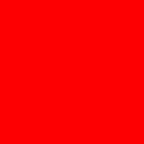


# Oracle Database Vault

# Oracle Database Vault

## Первое коммерческое решение для БД

- Позволяет исключать (ограничивать) доступ администраторов/суперпользователей к данным приложений (**keys to the kingdom**)
- В том числе:
  - ✓ контролировать доступ к приложениям и данным любого пользователя БД
  - ✓ определять привилегии пользователей согласно служебным обязанностям
  - ✓ проводить аудит действий, формировать отчеты
- Обеспечивает возможность безопасной консолидации IT-ресурсов организации
- Все механизмы “встроены” в БД Oracle



“Microsoft, IBM и Sybase не имеют  
аналогичных средств”

” Руководителям организаций важно,  
чтобы администраторы баз данных  
управляли базами данных, а **не данными** ...”



# Oracle Database Vault

## Функциональные элементы

Защищенные области

Отчеты

Многофакторная  
авторизация

Аудит

Динамическая  
настройка правил безопасности

Разграничение  
по служебным обязанностям

# Oracle Database Vault

Автоматизация превентивной защиты



# Oracle Audit Vault

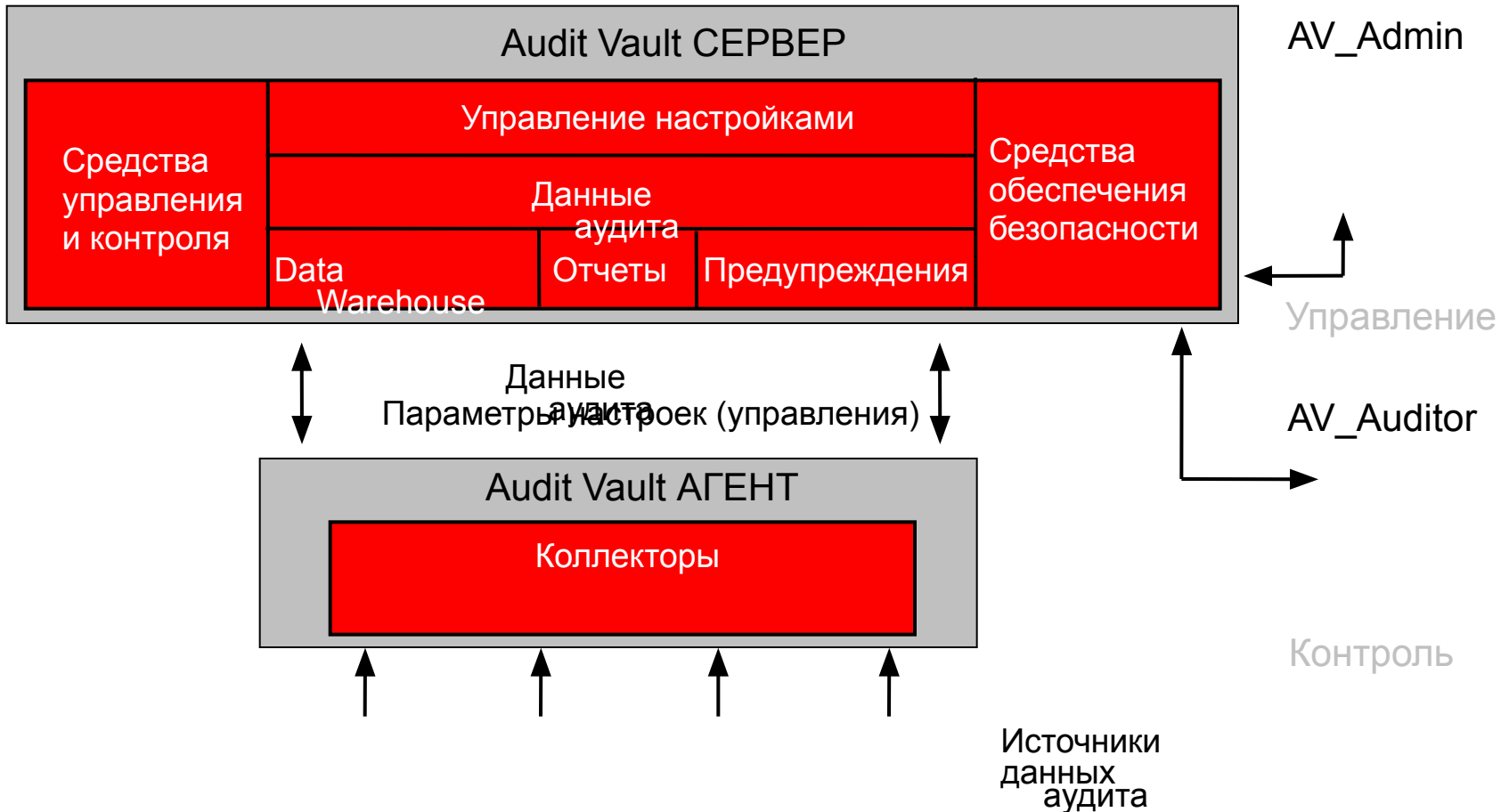
# Enterprise Auditing

## Требования пользователей

- **Консолидация данных аудита**
  - Много разрозненных данных (audit silos)
- **Отчеты по данным аудита**
  - Необходимость в специализированных отчетах для аудиторов
- **Мониторинг данных аудита**
  - Необходимость в эффективном и централизованном сканировании данных
- **Управление данными**
  - Обеспечение безопасного хранения конфиденциальных данных аудита
  - Большой объем хранимой информации
  - Архивирование данных
- **Настройка параметров аудита**
  - Необходимо обеспечить контроль и управление настройками параметров мониторинга и аудита

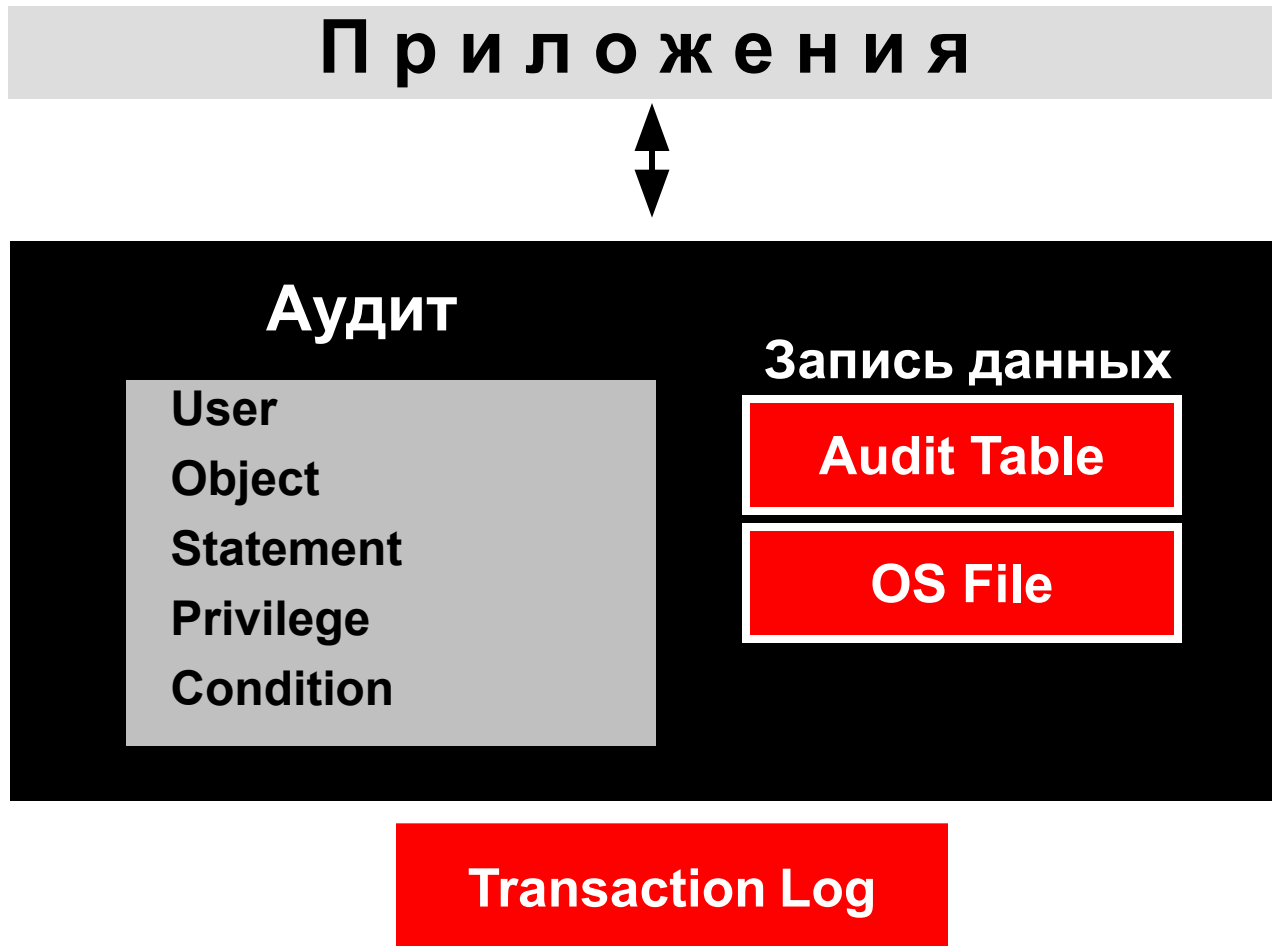
# Компоненты Audit Vault

## Функциональная схема



# Аудит в базах данных Oracle

Высокая точность и гибкость



# Преимущества использования **Audit Vault**

- Консолидация данных аудита, поступающих из различных прикладных систем
- Обнаружение изменений данных пользователями этих систем (в т.ч. и привилегированными)
- Защита получаемых данных аудита от изменений и других видов вмешательства
- Централизованное назначения политик аудита для баз данных Oracle

# Пользователи базовых решений

«Прозрачное»  
шифрование (TDE)

Мандатный доступ (OLS)

Виртуальные базы  
данных (VPD)

Шифрование трафика (ASO:Network encryption)

Шифрование данных (ASO:Encryption API)





**Решения Oracle по безопасности существенно  
способствуют выполнению Закона о  
персональных данных**

119435, Россия, Москва, Саввинская набережная, 15  
+7 (495) 641-1400 [Dmitry.Shepelyavy@oracle.com](mailto:Dmitry.Shepelyavy@oracle.com)