**Конференция**
**«Эффективные решения Oracle для бизнеса»**

**город Ростов-на-Дону,**
**23 марта 2011 года**

ORACLE®

UBTec
UNIVERSAL BUSINESS TECHNOLOGIES
ТЕХНОЛОГИИ МЕНЯЮТ МИР

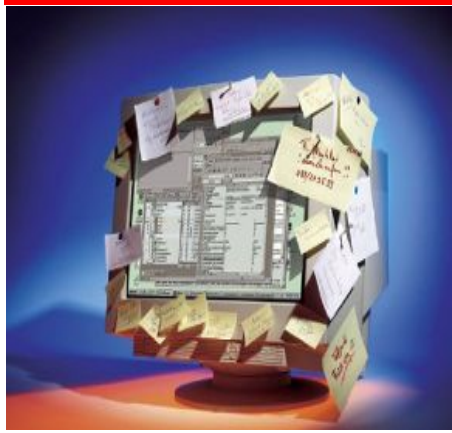
# Обеспечение информационной безопасности с помощью решений Oracle для российских заказчиков

Андрей Гусаков, ведущий системный архитектор Oracle EE/CIS

# План презентации

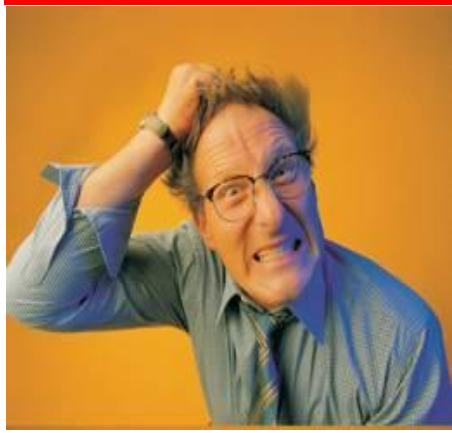
- Вопросы информационной безопасности и эволюция законотворчества в нашей стране
- Предложение Oracle – сквозная всеобъемлющая безопасность информации
- Защита информации на уровне СУБД и в электронных документах
- Oracle Identity Management – универсальный “зонтик” для защиты приложений
- Сертифицированные решения Oracle в области информационной безопасности для российских заказчиков
- Финансовые аспекты при планировании внедрения решений по защите информации

# Общие проблемы: управление рисками IT-безопасности



- Возрастающие объем данных и угрозы их компрометации
- Фрагментированные политики безопасности
  - «Сиротские» учетные записи
  - Отставание обновлений политик
  - Отсутствие агрегированного аудита и отчетности
- Изощренные интеллектуальные атаки
  - Эволюция преступных намерений
- Предрасположенные к ошибкам неавтоматизированные заявки на доступ
- Организационные и ролевые изменения требуют отражения в IT-привилегиях

# Общие проблемы: операционная эффективность



- Стоимость администрирования
  - Управление доступом десятков тысяч пользователей
  - Лавина обращения в службу поддержки
  - Ручное создание учетных записей для новых сотрудников
  - Ручная проверка данных аудита и построение консолидированных отчетов
- Продуктивность пользователей
  - Долгое получение доступа к запрошенным системам
  - Забытые пароли
- Продуктивность IT
  - Разработчики повторно разрабатывают политики безопасности для каждого приложения

# Общие проблемы: соблюдение законодательства

- Возрастающие требования регуляторов
- Несоответствие обходится дорого
- Недостатки некомплексных неустойчивых решений
  - Задержки при приеме на работу / увольнении
  - Непонятные привилегии
  - Конфликты прав доступа пользователей (например, к системам Закупок и Платежей)
  - Парольные политики действуют не во всех системах

# Эволюция законотворчества в нашей стране

- От требований для госструктур и тех, кто обеспечивает госзаказ (например, ДСП-приказ Гостехкомиссии России от 30.08.2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации [СТР-К]» к требованиям для всех (например, Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»)

  http://www.fstec.ru/_docs/_perech1.htm  http://www.rg.ru/gazeta/2006/07/29.html

- От общих рассуждений (например, Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации») к конкретным рекомендациям (например, Приказ ФСТЭК России от 5.02.2010 г. № 58 «Положения о методах и способах защиты информации в информационных системах персональных данных» и Комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» от 21.06.2010 г.)

  http://www.rg.ru/gazeta/2010/03/05.html  http://abiss.ru/news/337/

# Наиболее комплексный индустриальный набор документов в области безопасности,

СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.0-2010

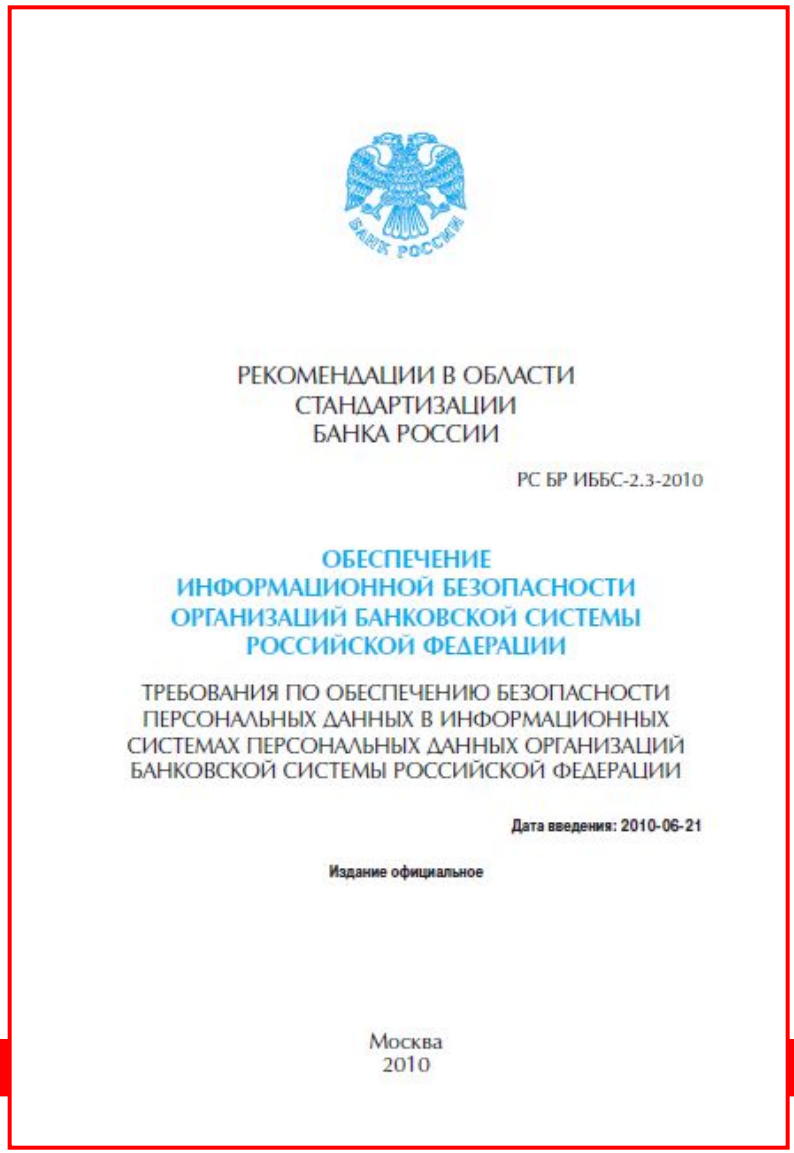
ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2010-06-21

Издание официальное

Москва
2010



РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.3-2010

ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ
СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИЙ
БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дата введения: 2010-06-21

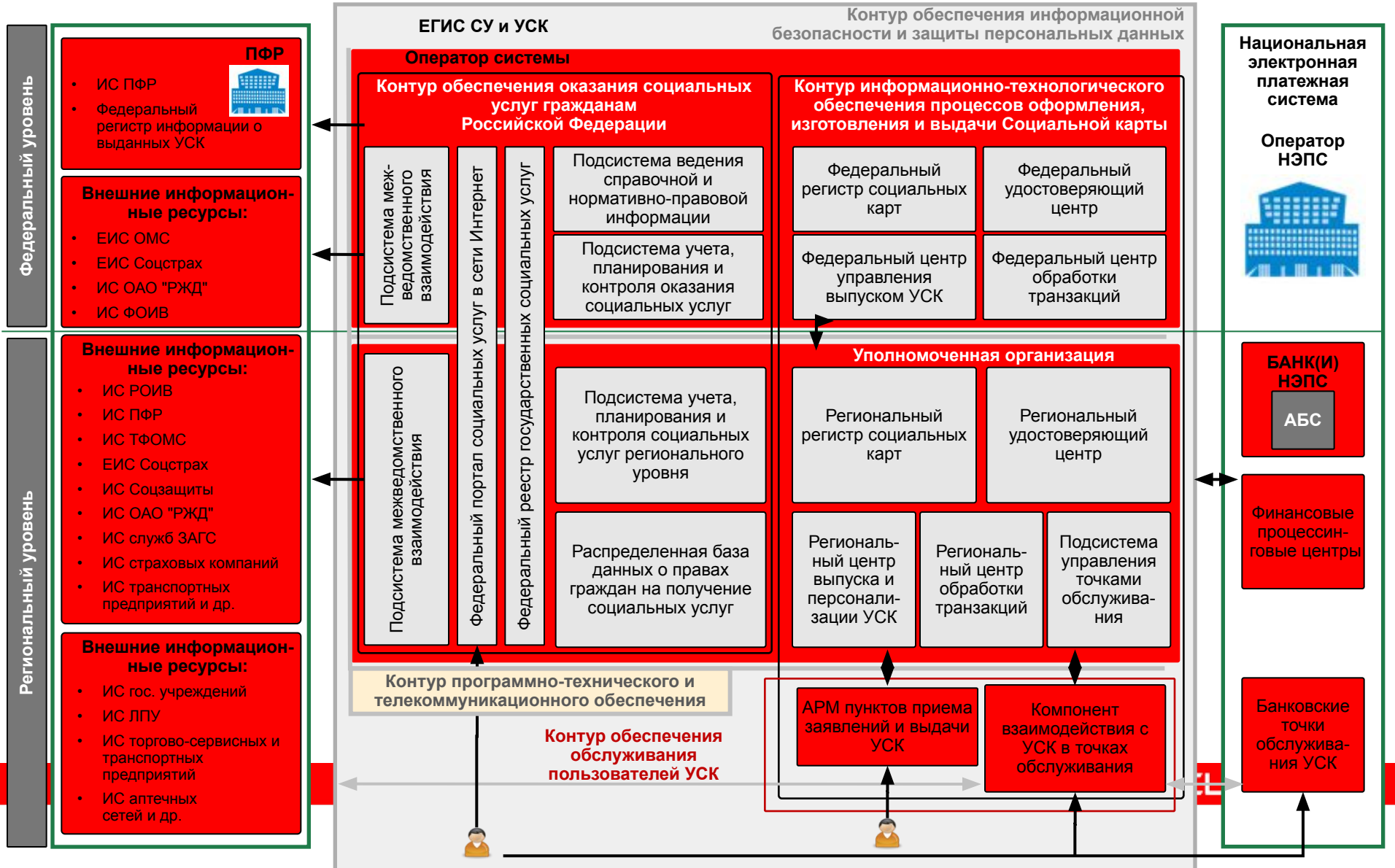
Издание официальное

Москва
2010

# …отвечающий современным тенденциям в области IT,…

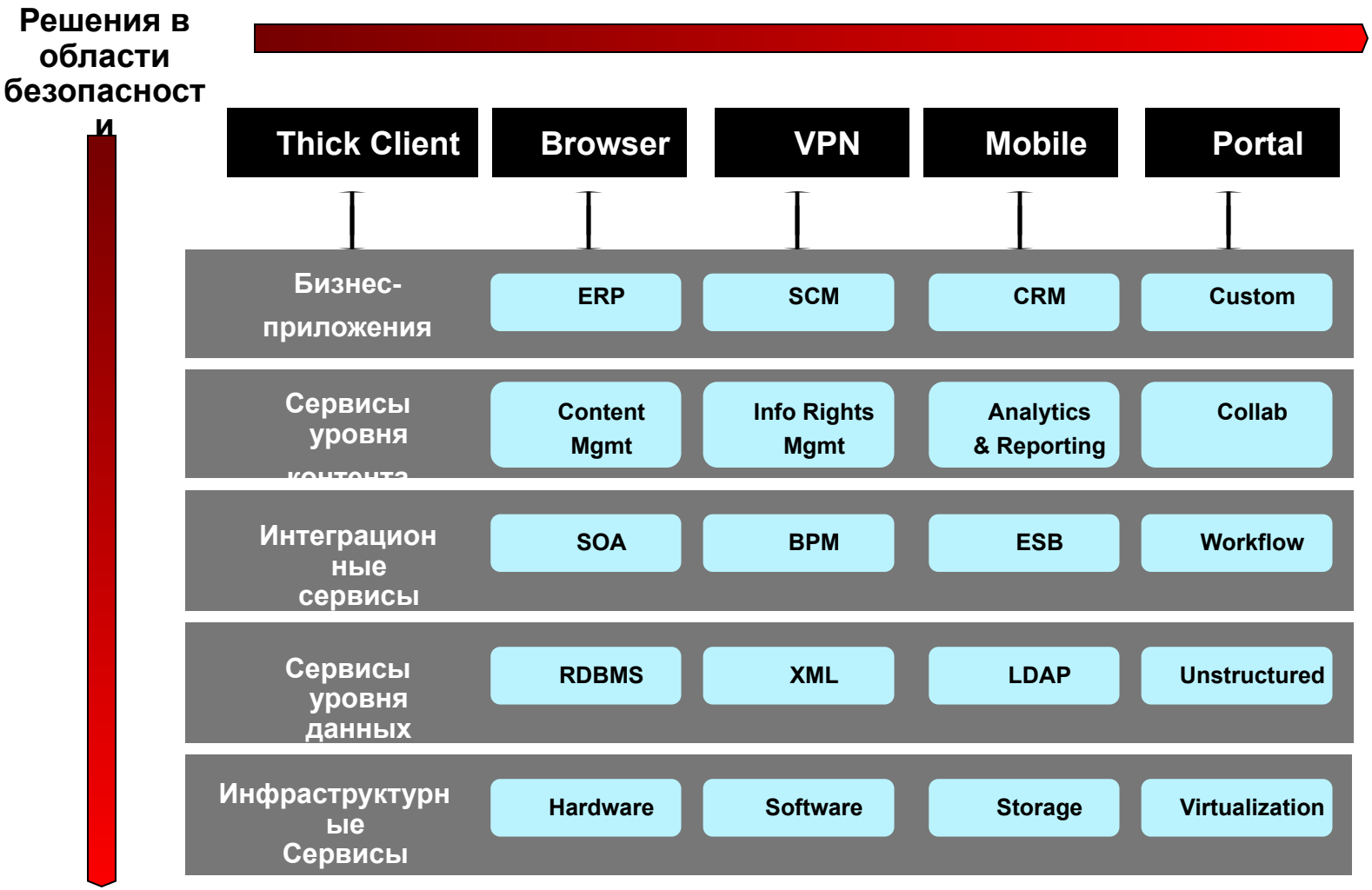
- Преобразование модели вычислений
  - Распределенные (облачные) и SaaS
  - Services-based Application Architecture
- Повышенное внимание к Extranet
  - Подтверждение идентификации и предотвращение краж
  - Масштабирование и производительность
- Консолидация инфраструктуры
  - Облегчение администрирования и оперативного управления
  - Упрощение интеграции за счет использования стандартов
- Управление на основе бизнес-процессов
  - Взаимодействие аналитических средств и решений для обеспечения информационной безопасности

# …масштабам крупных государственных проектов, например, «Соцкарта»…



# …и задачам крупных организаций

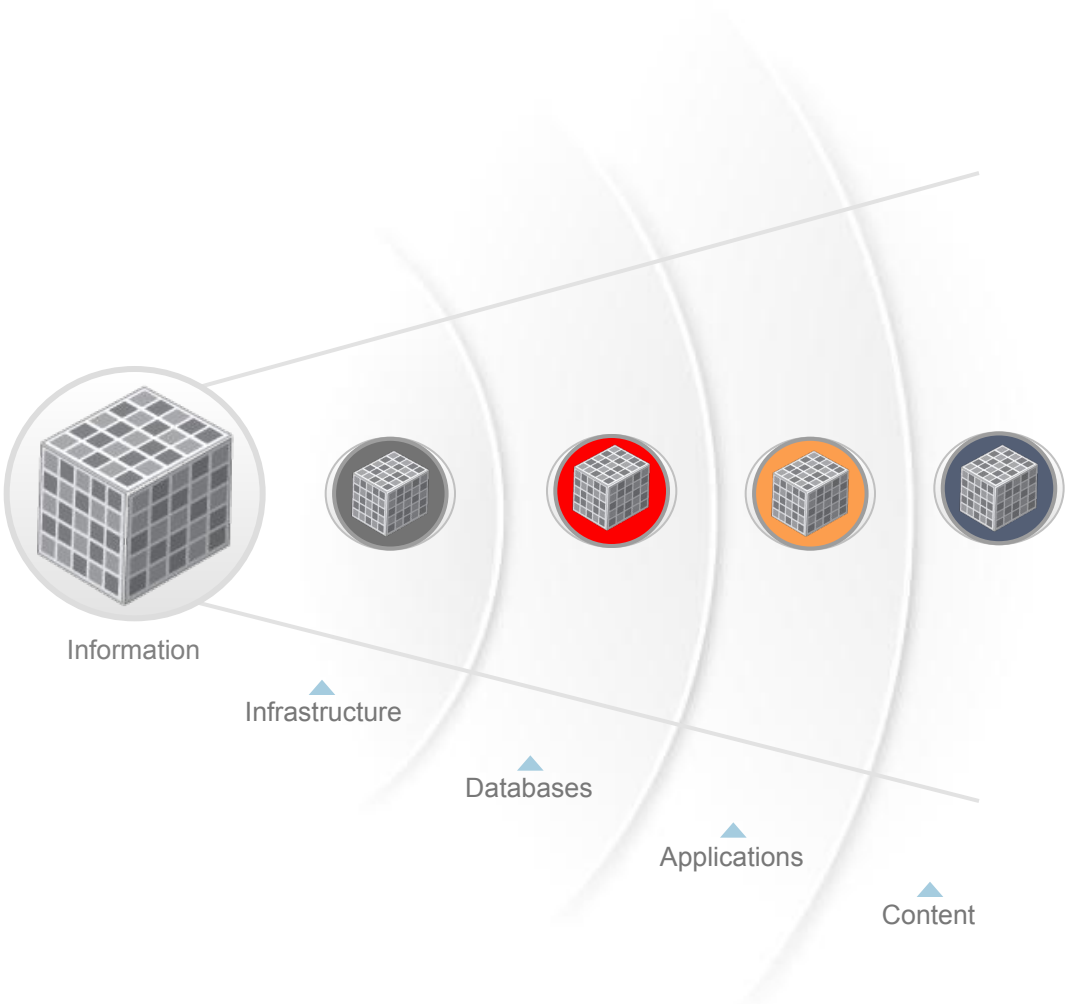
SECURITY INSIDE OUT
Oracle Security Solutions






ORACLE

# Внимание – защите информации




## Database Security

- Маскирование и преобразование
- Управление привилегированными пользователями
- Многофакторная авторизация
- Аудит и мониторинг активности
- Безопасное конфигурирование

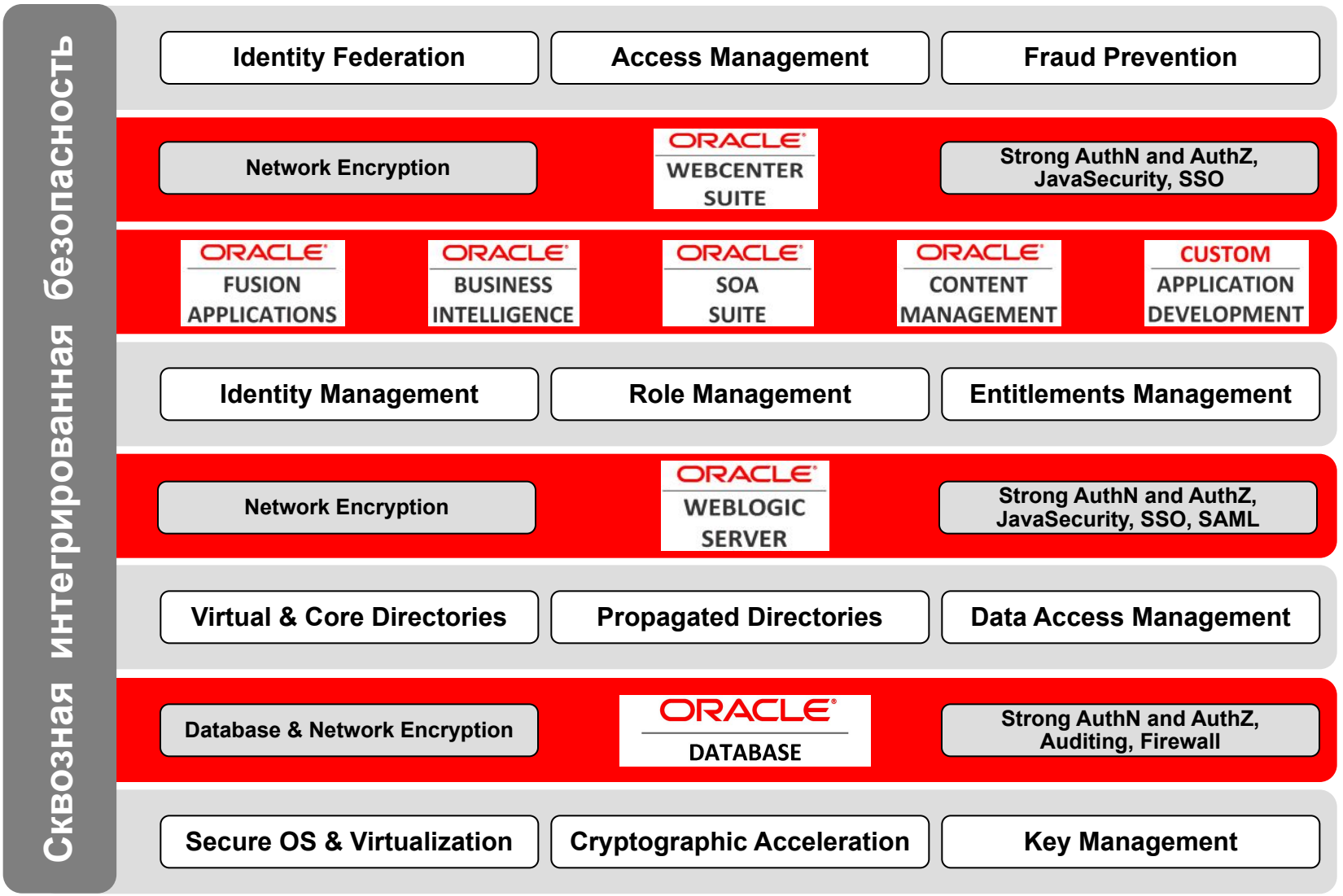
## Identity Management

- Назначение/отзыв IT-привилегий
- Управление ролями
- Универсальная авторизация
- Контроль доступа с учетом рисков
- Виртуальные каталоги

## Information Rights Management

- Аудит использования документов
- Предоставление и блокирование доступа к документам
- Безопасность документов внутри и вне межсетевых экранов

# Пример безопасного бизнес-приложения…

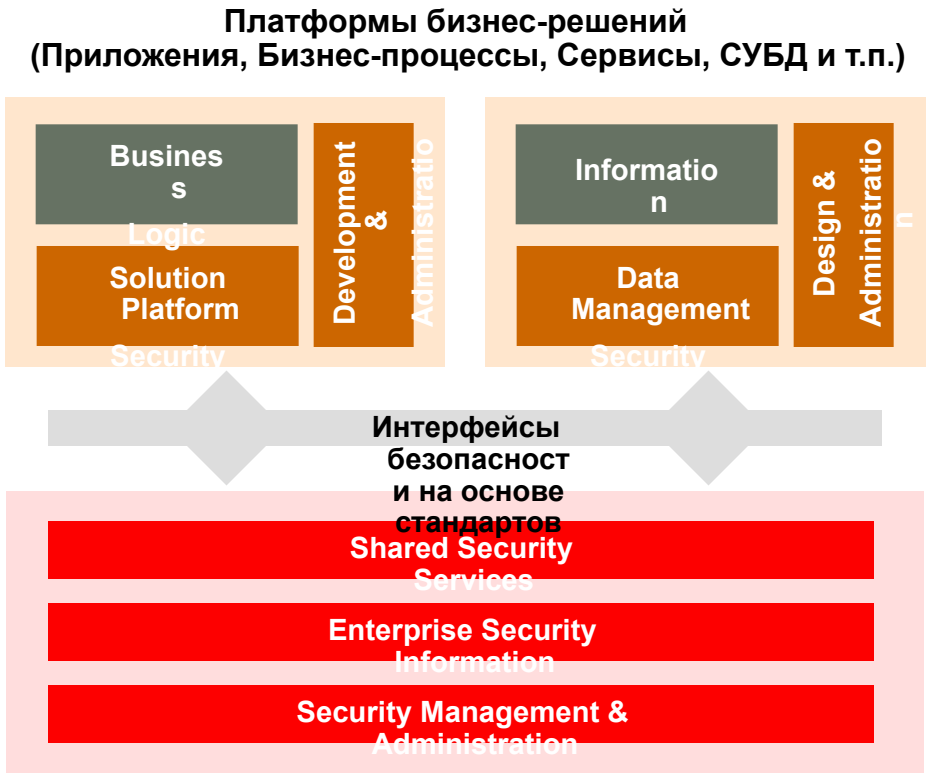





ORACLE

# …на основе референсной архитектуры Oracle

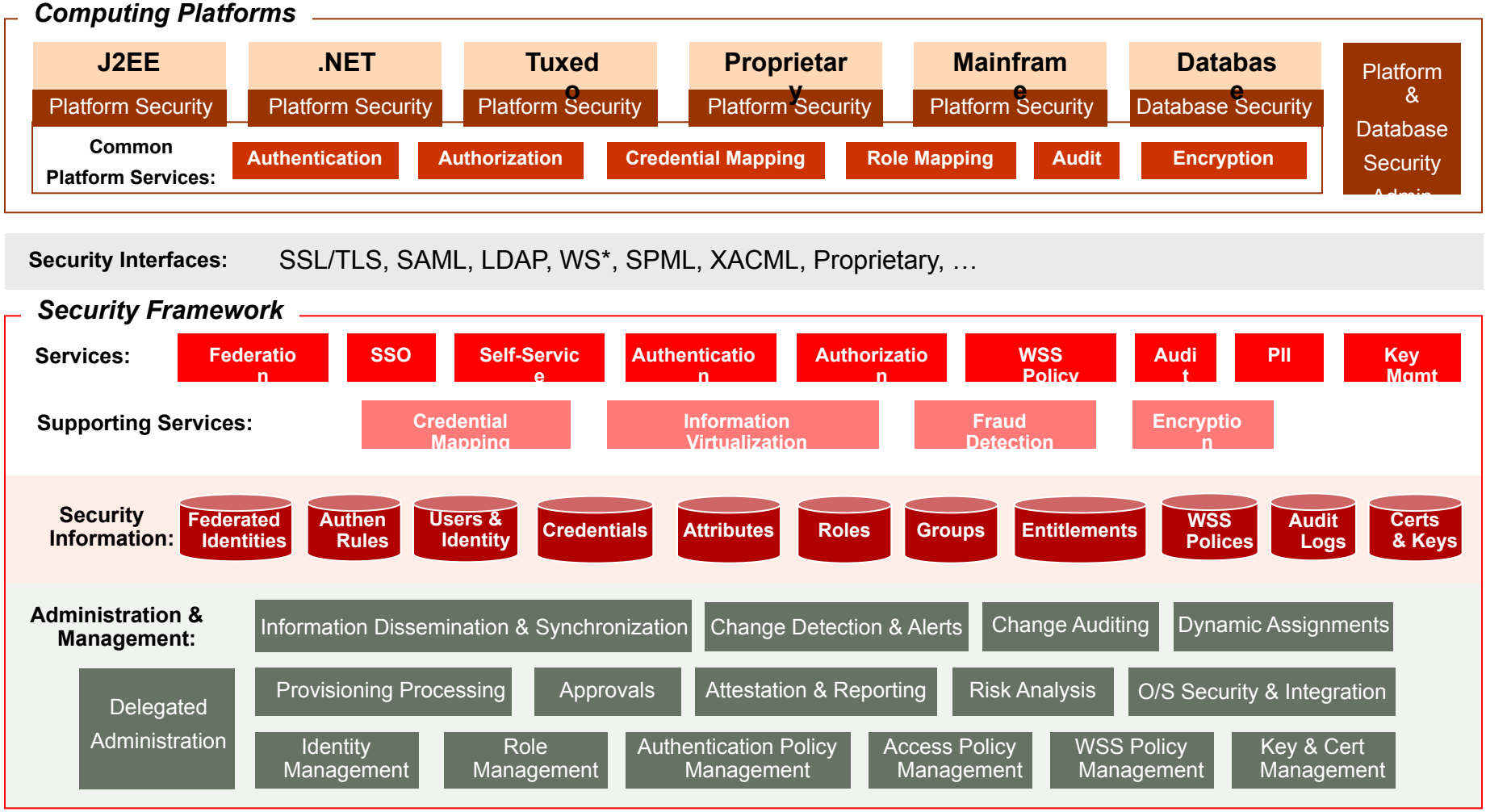
http://www.oracle.com/goto/itstrategies




**Oracle Security Reference Architecture**

http://oracle.com/technetwork/topics/entarch/oracle-ra-security-r3-0-176702.pdf

# Стандартизация интерфейсов облегчает интеграцию вычислительных платформ






ORACLE

# Полная поддержка стандартов и систем

**Отраслевые стандарты: Инновации, Вклад, Использование**








**Поддержка всех лидирующих приложений и систем**










ACF-2 & TSS


# Когда надо вспомнить про Oracle при построении СЗПДн

1. Определить ответственное структурное подразделение или должностное лицо
2. Определить состав обрабатываемых ПДн, цели и условия обработки, срок хранения
3. Получить (письменное) согласие субъекта на обработку его ПДн
4. Определить порядок реагирования на запросы со стороны субъектов ПДн
5. Определить необходимость уведомления уполномоченного органа по защите ПДн о начале обработки ПДн. Если необходимость есть, то составить и отправить уведомление
6. Выделить и классифицировать ИСПДн
7. Разработать модель угроз для ИСПДн
8. Спроектировать и реализовать СЗПДн
9. Провести аттестацию ИСПДн по требованиям безопасности или продекларировать соответствие
10. Определить перечень мер по защите ПДн, обрабатываемых без использования средств автоматизации
11. Выполнять постоянный контроль над обеспечением уровня защищенности ПДн

http://leta.ru/library/methodological/

http://leta.ru/library/methodological/

# Примеры информационных бизнес-активов

- Биллинг/АБС – важнейшая бизнес-система, содержит много конфиденциальной информации о клиентах
- ERP/HRMS – важнейшая бизнес-система, содержит много конфиденциальной информации о сотрудниках
- Система документооборота – важная бизнес-система, содержит много конфиденциальной информации
- Service Desk – важная бизнес-система, содержит конфиденциальную информацию
- Электронная почта – вспомогательная бизнес-система, содержит конфиденциальную информацию

# Примеры моделей угроз, оценка эффективности

- Биллинг/АБС – информация открыта для привилегированных пользователей, резервные копии не защищены, затруднен аудит привилегий
- ERP/HRMS – информация открыта для привилегированных пользователей, резервные копии не защищены, сложная система привилегий
- Система документооборота – уязвимость извлеченных данных, затруднен аудит привилегий
- Service Desk – проблема точности выполнения заявок, задержки согласования
- Электронная почта – необходимость повторной аутентификации при web-доступе

# Защита структурированной информации в СУБД Oracle и электронных документов

# Технологии защиты информации

- Авторизованный доступ
  - dB, ASO (аутентификация), EUS (интеграция DB с IAMS), IRM
- Фильтрация (сокрытие) информации
  - dB, VPD, OLS, DBV
- Криптопреобразование информации
  - ASO – в базе, в архиве, в сети
  - Secured Backup, Data Masking
  - IRM
- Активный мониторинг доступа
  - DBV, DBFW
  - IRM, OAM (из IAMS)
- Аудит и расследование инцидентов
  - Вышеперечисленное, Audit Vault, OIM, OAAM

# Защита СУБД Oracle с помощью ASO

- ASO = Advanced Security Option
- Опция Oracle Database EE
- Пакет из трех компонентов:
  - TDE (Transparent Data Encryption) для объектов СУБД / файлов / резервных копий
  - Network Encryption
  - средства строгой аутентификации Kerberos / PKI / RADIUS
- Опция интегрирована на уровне ядра для всех СУБД версий 10g / 11g
- Не требуется модификация структуры СУБД или приложения; сохраняется индексация

http://www.oracle.com/global/ru/pdfs/data/security/oracle_advanced_security.pdf

# ASO: Защита на физическом уровне

## Прозрачное шифрование

Зашифровывание данных при записи

Расшифровывание данных при чтении

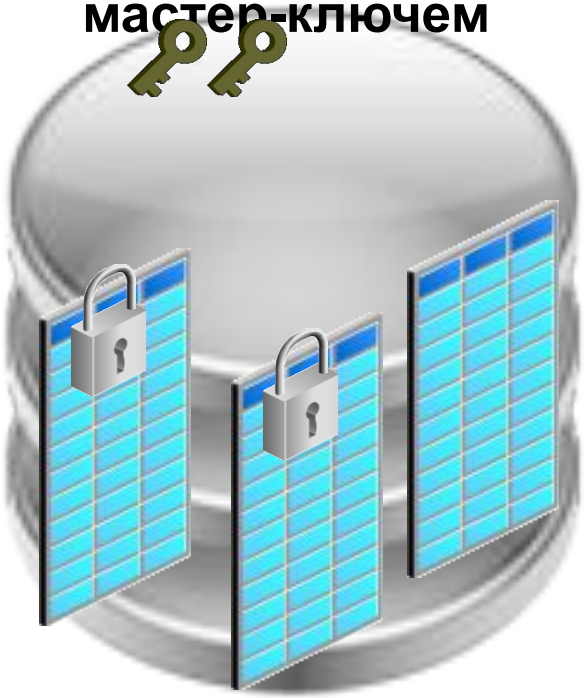
**Данные на физических носителях информации и в резервных копиях защищены**

# ASO: Ключи прозрачного шифрования

## Мастер-ключ и ключи защищенных колонок

Ключи для колонок защищены мастер-ключем

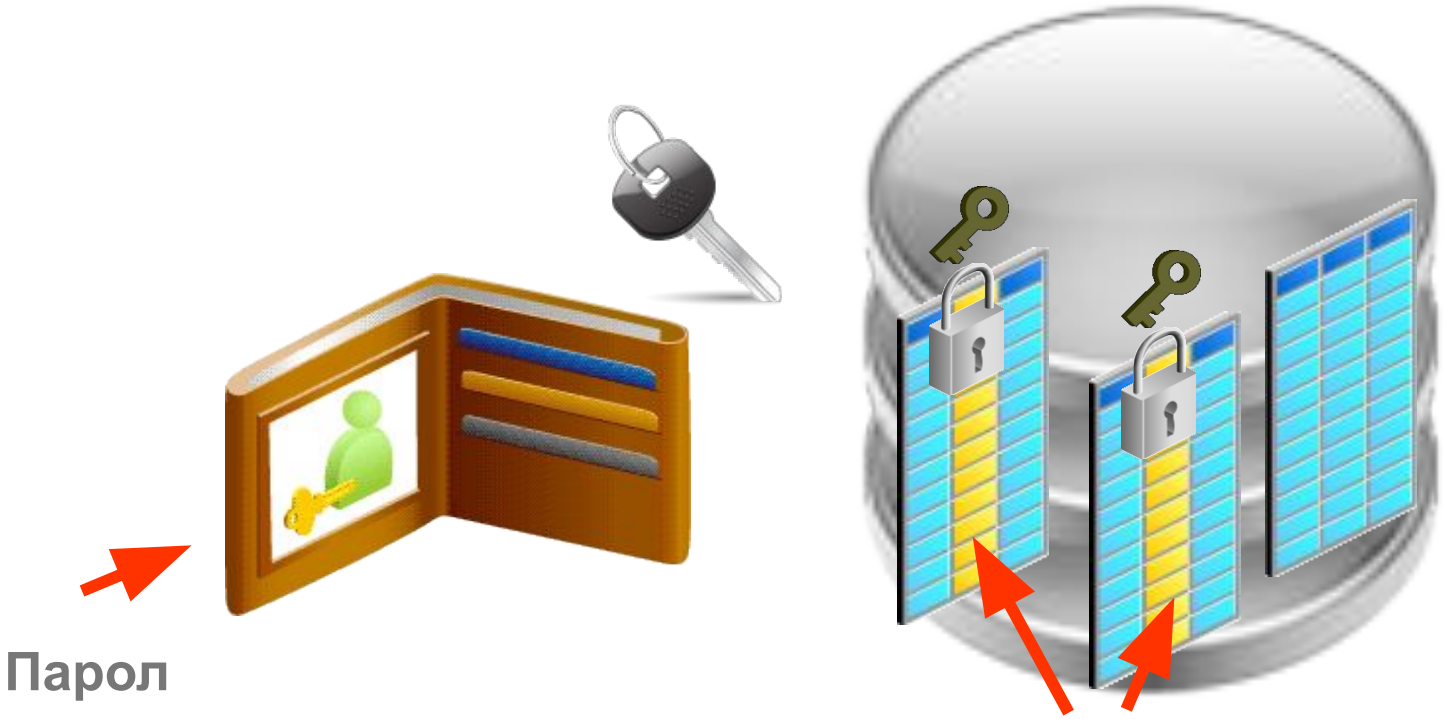
Мастер-ключ хранится в PKCS#12 wallet



Таблицы с защищенными колонками

# ASO: Ключи прозрачного шифрования

## Доступ к данным разрешен



# ASO: Управление правами доступа

## Разделение обязанностей

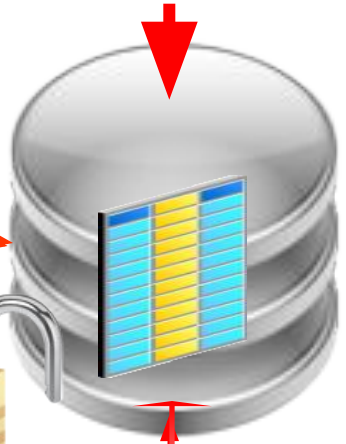
# ASO: Права доступа к работающей СУБД

## Обеспечение доступа клиентов и его некоторые неприятные особенности

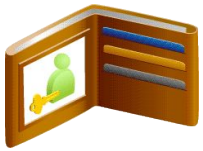
SELECT ANY TABLE

Database
DBA

Доступ к данным разрешен всем…



Паро
ль



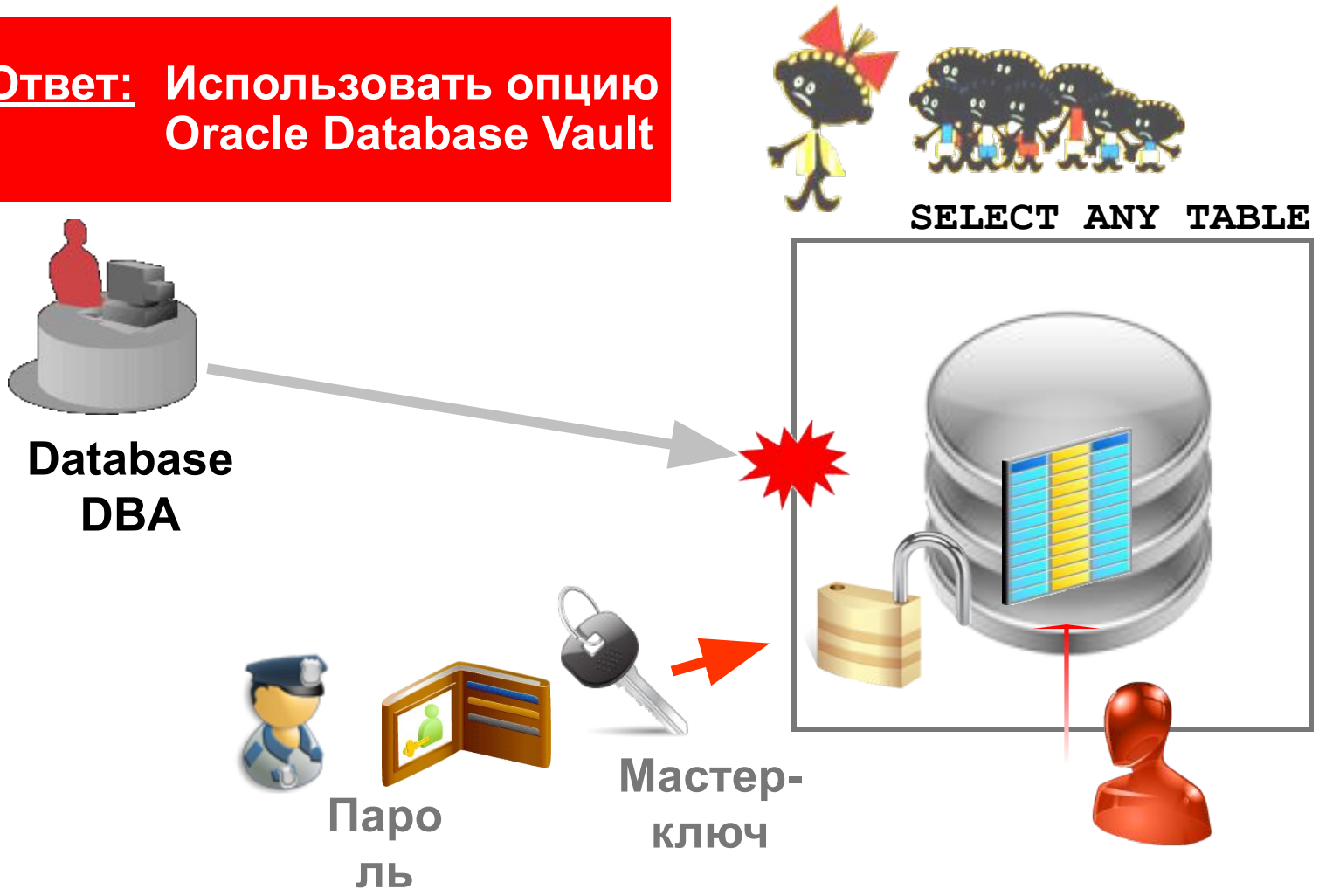
Мастер-
ключ

Доступ к данным разрешен

# ASO: ограничения на работающей СУБД

## Как защитить данные от инсайдеров ?

**Ответ:** Использовать опцию Oracle Database Vault

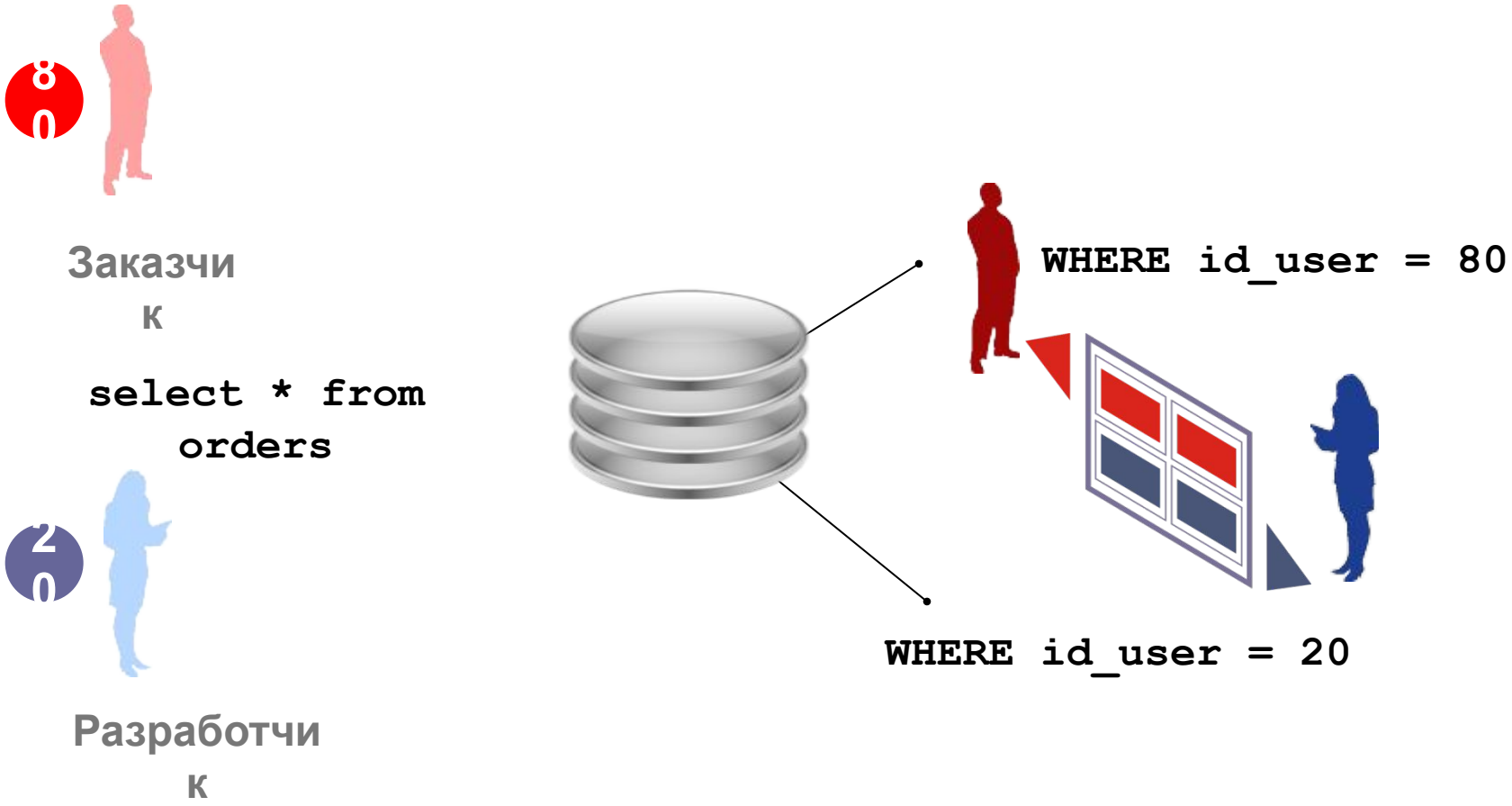





ORACLE

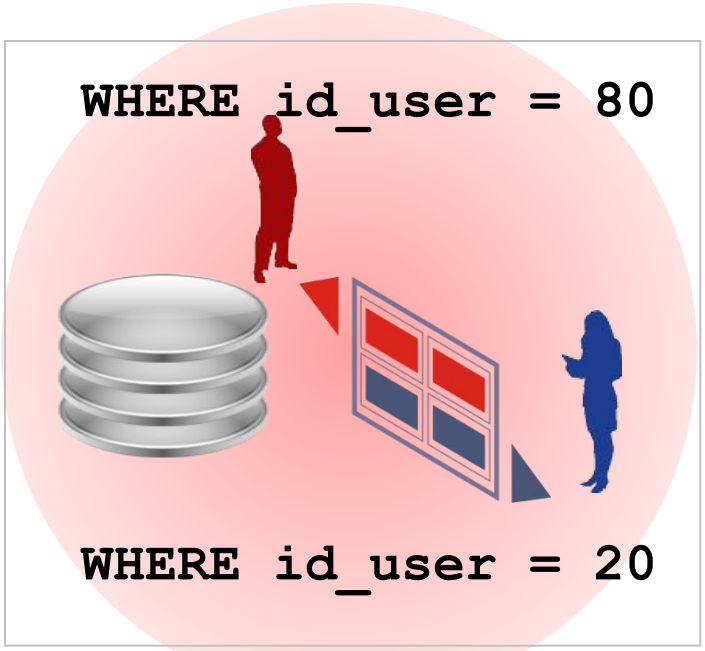
# Как обеспечить доступ только к своим данным?

## Вариант 1: Виртуальные базы данных (VPD)



# Недостаток виртуальных базы данных

**Как обеспечить более сложные правила ?**




**Простое правило с использованием значения идентификатора пользователя**

**Учесть степень (уровень) конфиденциальности данных**

**Разделить данные по категориям**

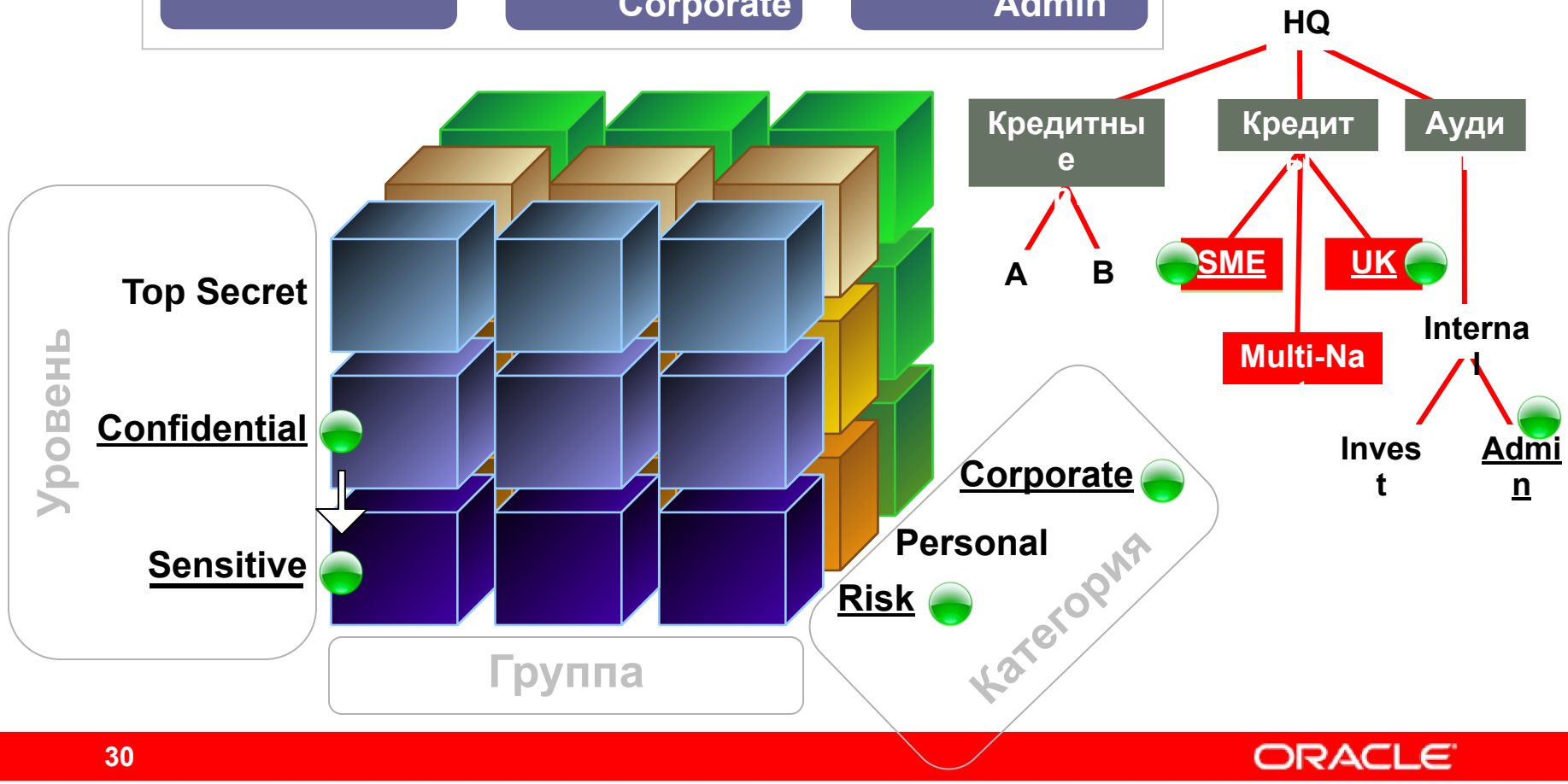
**Обеспечить обработку данных только теми сотрудниками организаций, которые владеют данными или имеют к ним доступ**

**Ответ:** **Использовать опцию Oracle Label Security**

# Как обеспечить доступ только к своим данным?

## Вариант 2: Комбинации меток (OLS)

**Добавляются уровни, категории и иерархии**

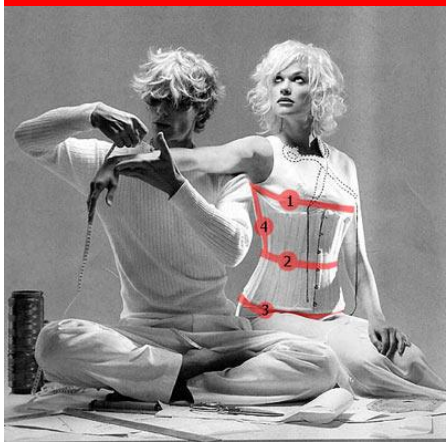






ORACLE

# Как обеспечить доступ только к своим данным?

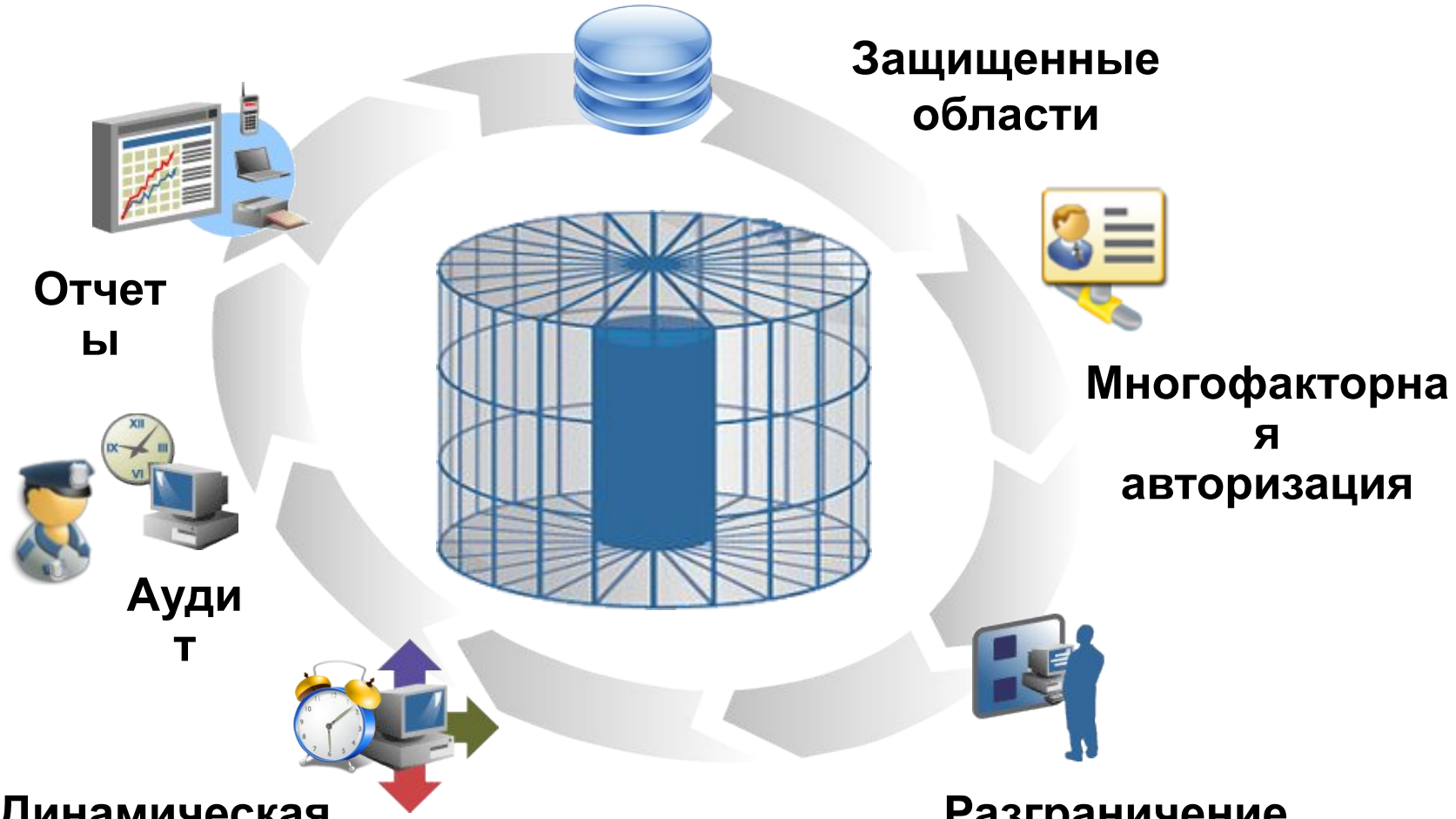
## Вариант 3: политики Oracle Database Vault




- Опция СУБД Oracle 10g Release 2 EE
  Oracle 11g Release 2 EE
  или Oracle 9i R2 (9.2.0.8) EE
- Возможность ограничивать (исключать) доступ к данным приложений со стороны администратора базы данных (DBA)
- Обеспечение доступа к данным на основе динамически настраиваемых правил
- Повышение защищенности объектов БД от несанкционированных изменений
- Разделение полномочий пользователей в соответствии с их функциональными обязанностями и надежный внутренний контроль

# Oracle Database Vault

## Функциональные элементы

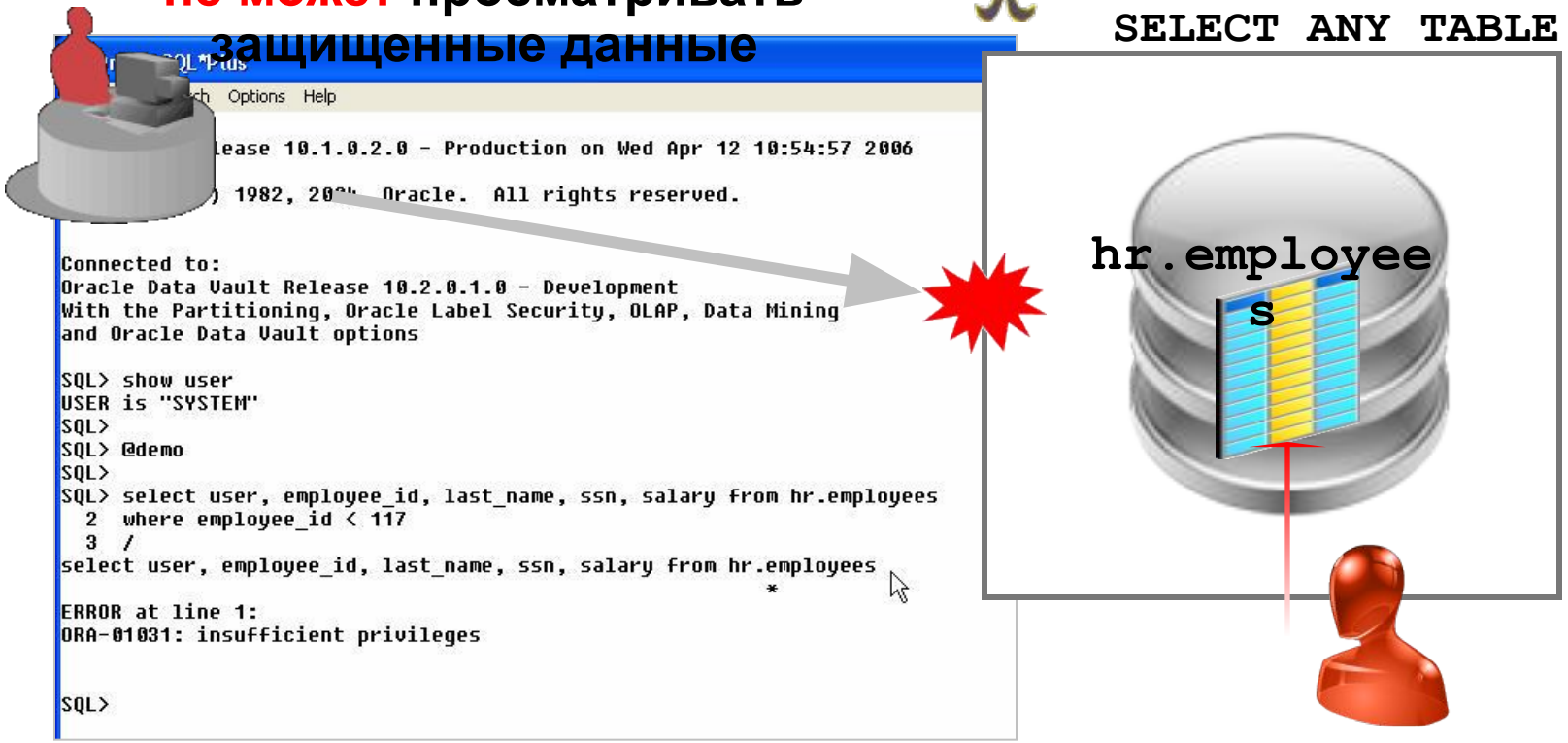


# Защищенная область Oracle Database Vault

## Результат применения

**Даже пользователь SYSTEM не может просматривать защищенные данные**

SELECT ANY TABLE






ORACLE

# Oracle Database Vault

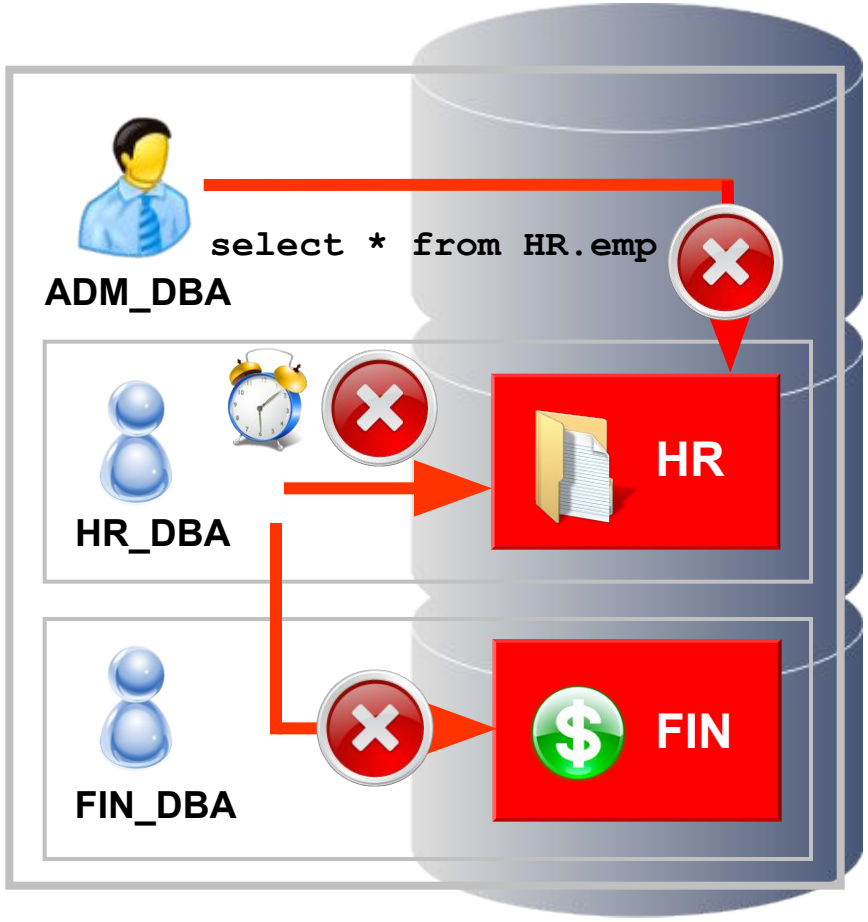
## Пример использования

- **Администратор БД (ADM_DBA) обращается к данным в схеме HR**

**Соответствие нормативным требованиям и стандартам внутреннего аудита**

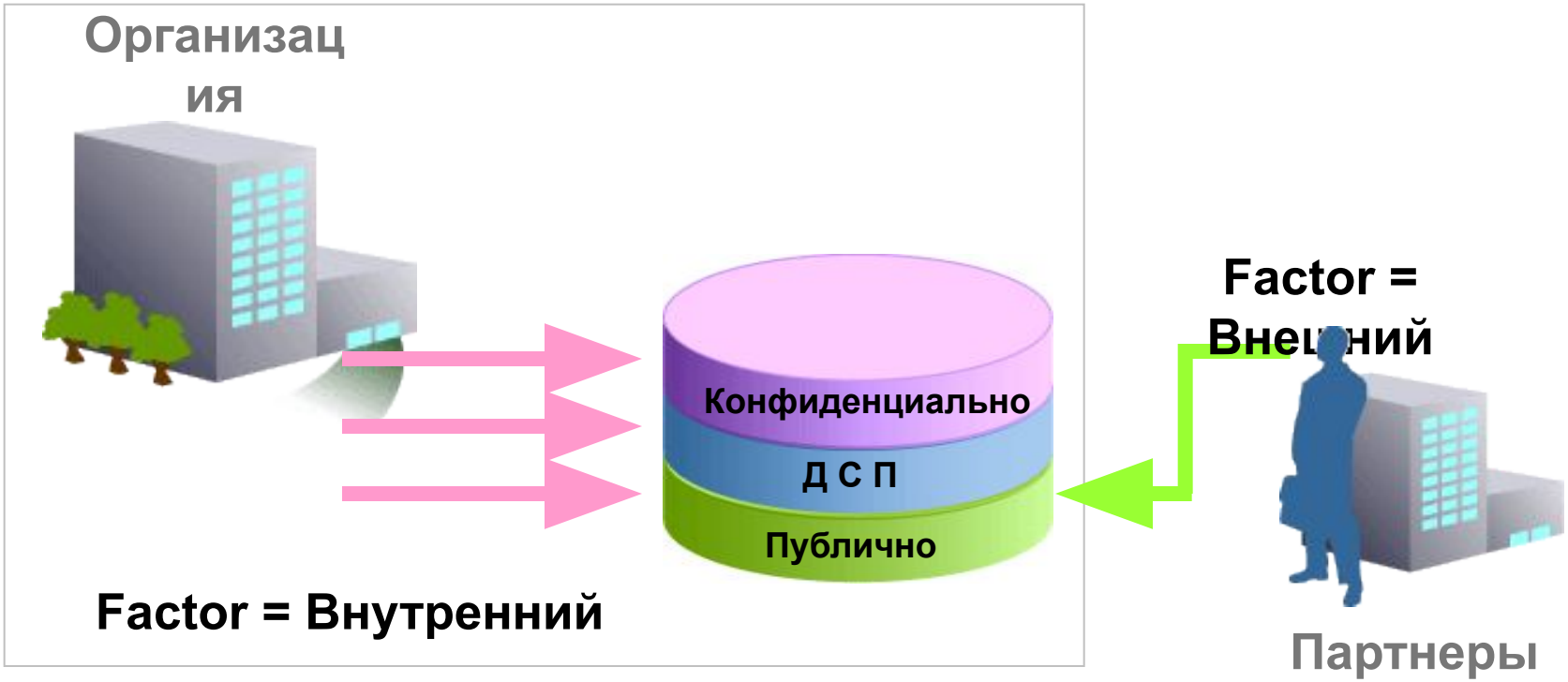
- **Пользователь HR_DBA обращается к данным в схеме FIN или желает получить доступ к области HR во внерабочее время**

**Безопасная консолидация приложений на одном сервере**



# Многофакторная авторизация

## Интеграция с Oracle Label Security




**Oracle Label Security ограничивает доступ к данным на основе факторов Database Vault**

# Oracle Database Vault

## Отчеты и аудит

ORACLE Database Vault

Database

Database Instance: dvault.lowenthal.vm > Report Results: Realm Audit

### Report Results: Realm Audit

Page Refreshed **Jun 13, 2006 12:17:32 PM**

Return To Reports Menu

Previous 1-25 of 598 Next 25

| Violation Attempt | Timestamp | Return Code | Account | User Host | Instance Number | Realm Name | Rule Set | Command |
|---|---|---|---|---|---|---|---|---|
| Realm Violation Audit | JUN 13, 2006 11:16:04 A.M. | 1031 | HR | DATAVAULT | 1 | HR_shema | | |
| Realm Violation Audit | JUN 13, 2006 11:13:11 A.M. | 1031 | HR | DATAVAULT | 1 | HR_shema | | |
| Realm Violation Audit | JUN 13, 2006 09:32:46 A.M. | -47401 | BERNST | DATAVAULT | 1 | HR_shema | | drop table hr.employees_copy |
| Realm Violation Audit | JUN 13, 2006 09:30:45 A.M. | -47401 | BERNST | DATAVAULT | 1 | HR_shema | | |
| Realm Violation Audit | JUN 13, 2006 08:59:19 A.M. | -47401 | SYSTEM | DATAVAULT | 1 | Oracle Data Dictionary | | grant dba to hr_dba |

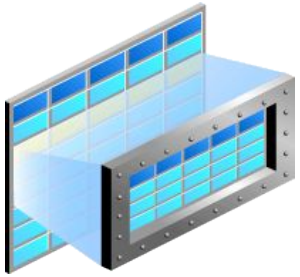
Factor Audit



ORACLE

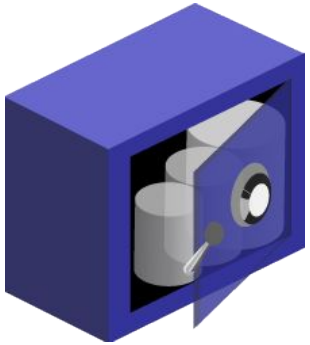
# В чем отличие DBV от VPD и OLS

- Virtual Private Database (VPD):
  - Ограничивает доступ пользователя к определенным строкам на основе параметра **`WHERE`**



- Oracle Label Security (OLS):
  - Определяет доступ пользователя к определенным строкам на основе меток строки и уровня его конфиденциальности

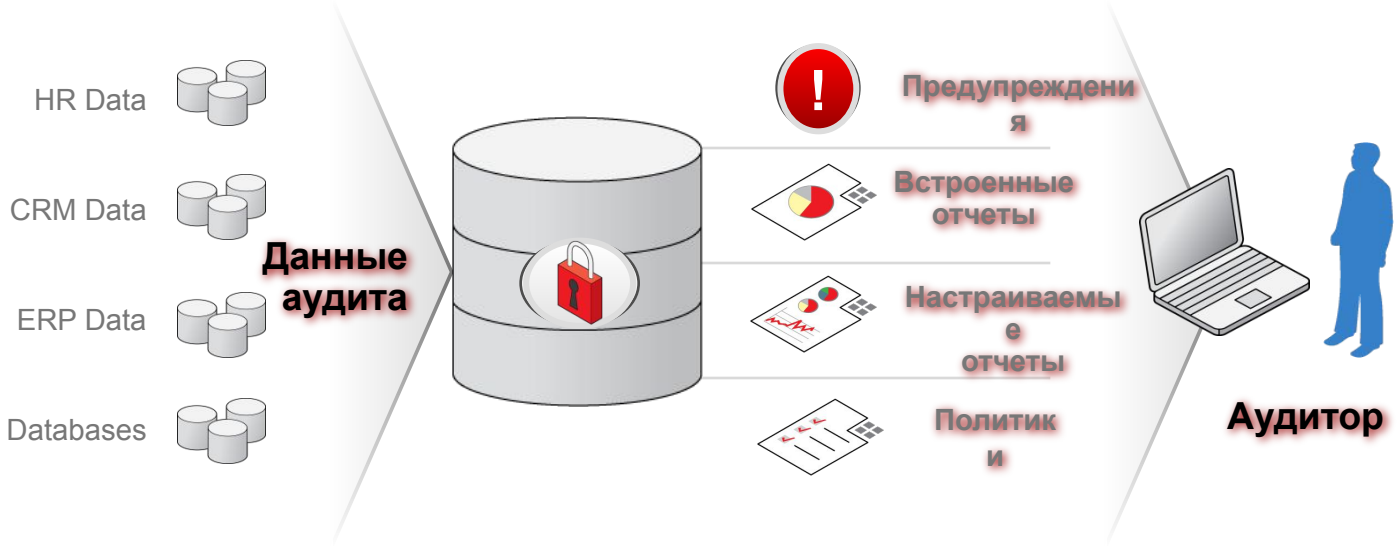
**VPD и OLS ограничивают доступ на уровне строк, в то время как Database Vault ограничивает доступ на уровнях объектов и команд**



http://www.oracle.com/global/ru/pdfs/tech/oracle-security.pdf

# Oracle Audit Vault

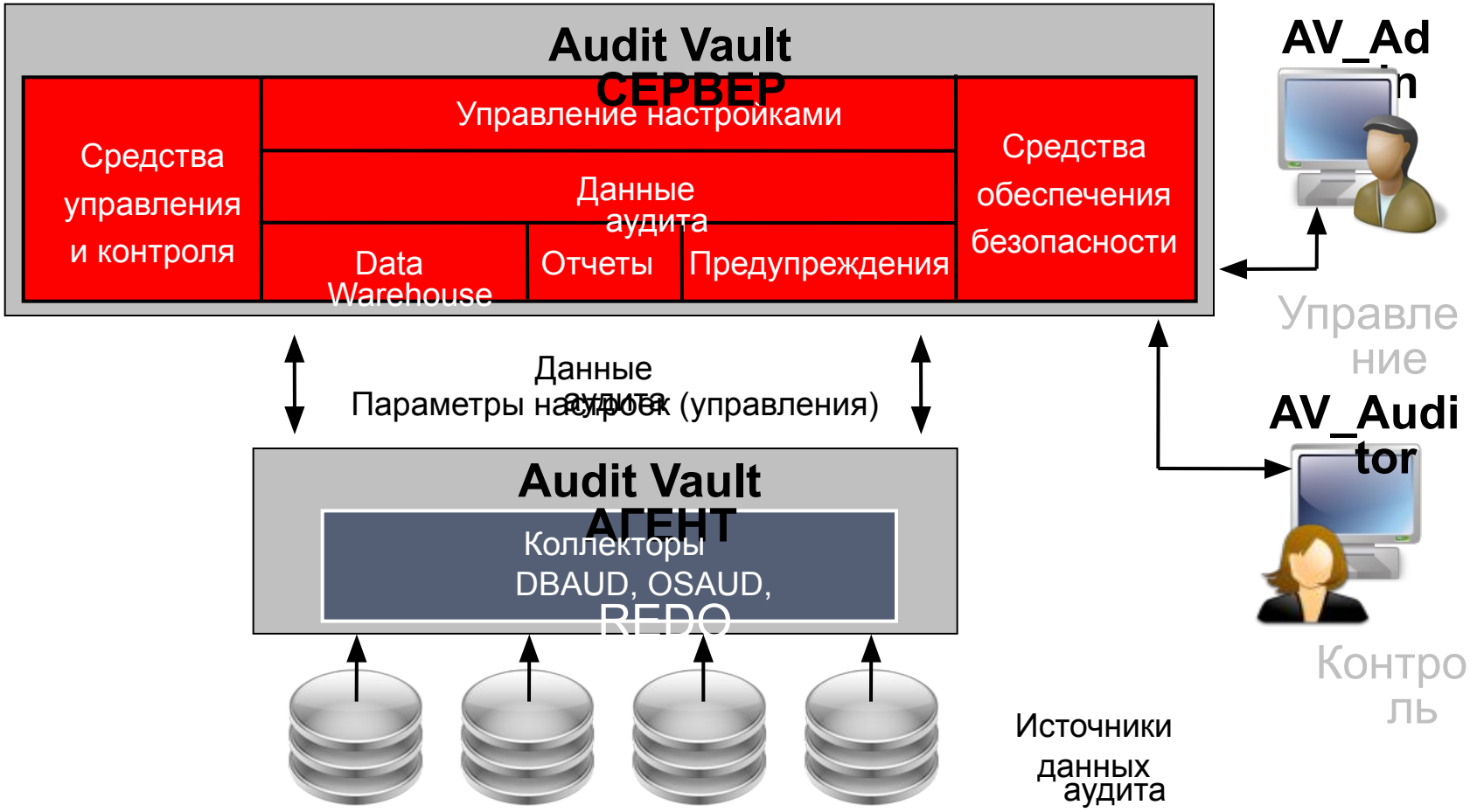
## Мониторинг и отчетность




- Консолидация данных аудита в защищенном хранилище
- Обнаружение подозрительной активности. Предупреждения
- Встроенные и настраиваемые  отчеты
- Централизованное управление политиками

# Oracle Audit Vault

## Функциональная схема






ORACLE

# Oracle Audit Vault

## Поддерживаемые базы данных

| СУБД | Версия | Данные аудита расположены |
|---|---|---|
| Oracle Database | Oracle Database 9iR2,<br>Oracle Database 10g,<br>Oracle Database 11g | • Таблицы стандартного и FGA аудита<br>• Записи в файлах ОС (XML, TXT) или SYSLOG<br>• Значения данных ДО и ПОСЛЕ обновления, изменения (DDL) из Redo Log<br>• Данные аудита, специфичные для Database Vault |
| Microsoft SQL Server | 2000, 2005, 2008 | • Server side trace<br>• Windows event<br>• C2 |
| IBM DB2 | 8.2, 9.1 & 9.5 on Linux, Unix, Windows | • Двоичные файлы ОС средств аудита |
| Sybase ASE | 12.5.4 - 15.0.x | • Sybsecurity таблицы БД |

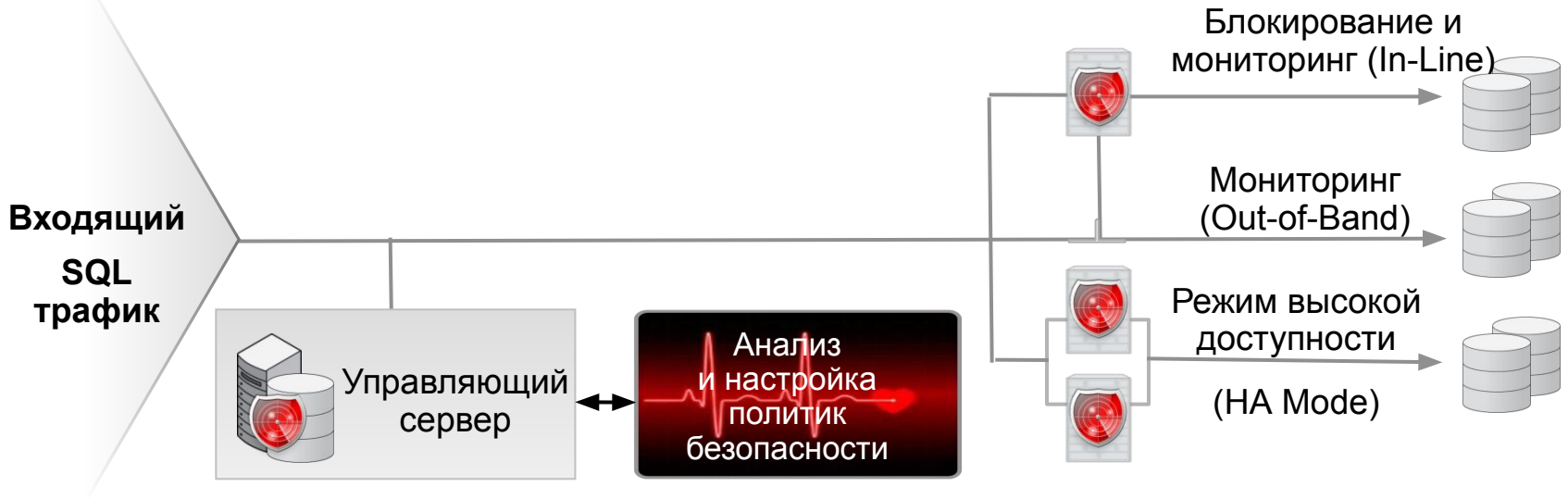
# Oracle Database Firewall

## Первый рубеж защиты базы данных


- **Мониторинг трафика и исключение неавторизованного доступа к базам данных**, исключение SQL инъекций, позволяющих не санкционировано повышать привилегии и получать доступ к конфиденциальным данным.
- Аккуратный грамматический анализ SQL выражений
- Высокая масштабируемость и производительность
- Встроенные отчеты для анализа соответствия нормативным требованиям

# Oracle Database Firewall

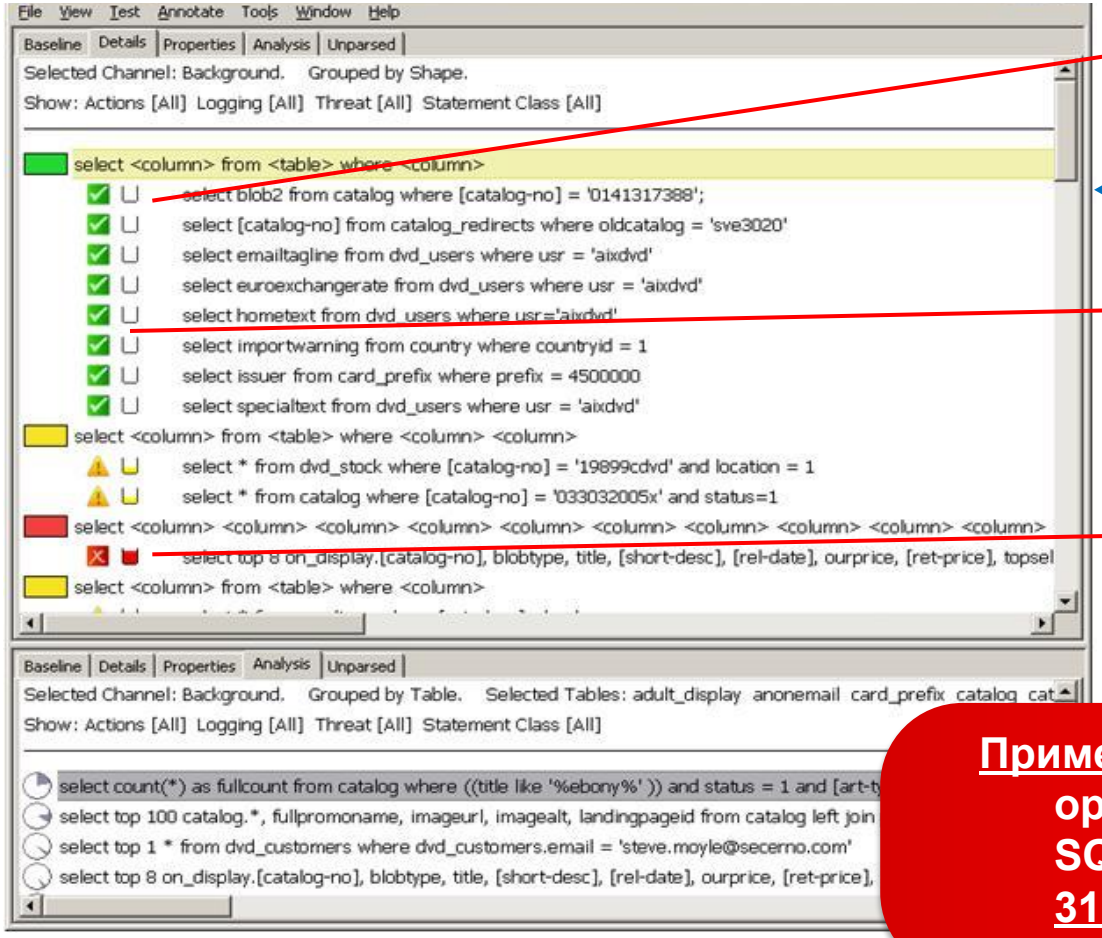
## Архитектура




- Режимы мониторинга с возможность блокирования или мониторинга
- Обеспечение высокой доступности
- Мониторинг удаленных баз данных путем перенаправления сетевого трафика
- Не зависит от используемых приложений
- Применим для СУБД Oracle и баз сторонних поставщиков

# Oracle Database Firewall

## Пример грамматической кластеризации




Кластеры по типам (intent)

```
select <column> from
<table> where <column>
```

В один и тот же кластер попадают запросы для выборки данных из различных таблиц БД

Специфические запросы фиксируются

**Пример: В финансовой организации для 57 млн. SQL выражений получено 310 кластеров**

# Oracle Database Firewall

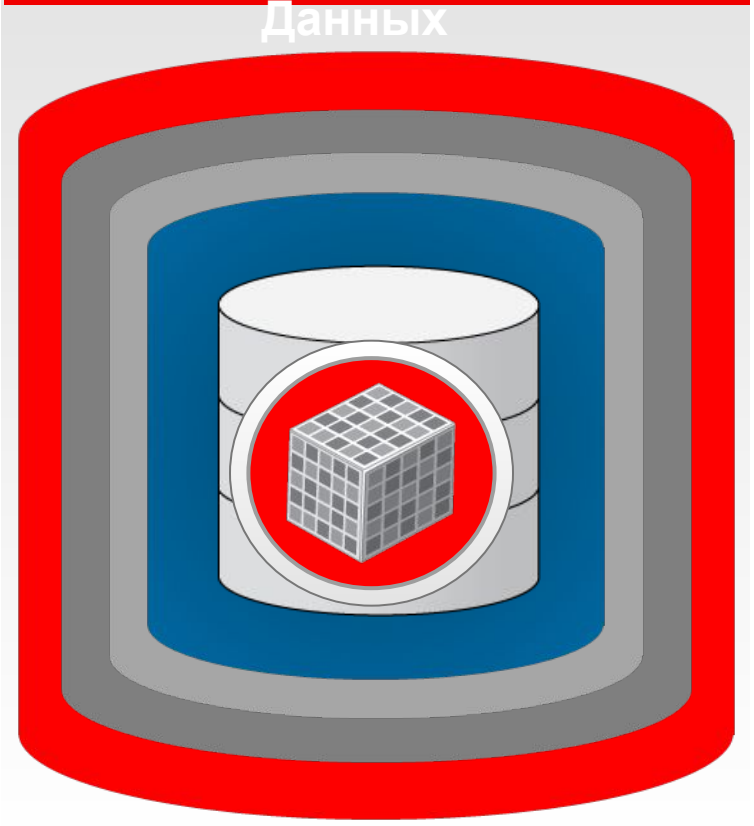
## Поддерживаемые базы данных

| | Oracle 8.1 - 11.2.x | Microsoft SQL Server 2000, 2005, 2008 | IBM DB2 for LUW 9.x | Sybase ASE 12.5.4 - 15.0.x | SQL Anywhere 10.x |
|---|---|---|---|---|---|
| SQL Monitoring | X | X | X | X | X |
| Blocking | X | X | X | X | X |
| Statement Substitution | X | X | - | X | X |
| User Role Monitoring (URA) | X | X | X | X | X |
| Stored Procedure Change Review (SPA) | X | X | X | X | X |
| Local Monitor | X | X | - | X | - |
| Remote Monitor (Linux Only) | X | - | X | X | X |
| Database Response Monitoring | X | X | X | X | X |

# Мнение IDC: Финансово эффективная защита от утечек данных начинается в СУБД

IDC
Analyze the Future

**Безопасность Баз Данных**



**Преобразование данных и маскирование**

Oracle Advanced Security
Oracle Secure Backup
Oracle Data Masking

**Контроль доступа к данным**

Oracle Database Vault
Oracle Label Security

**Контроль изменений и аудит**

Oracle Audit Vault
Oracle Configuration Management
Oracle Total Recall

**Мониторинг и блокирование трафика**

Oracle Database Firewall

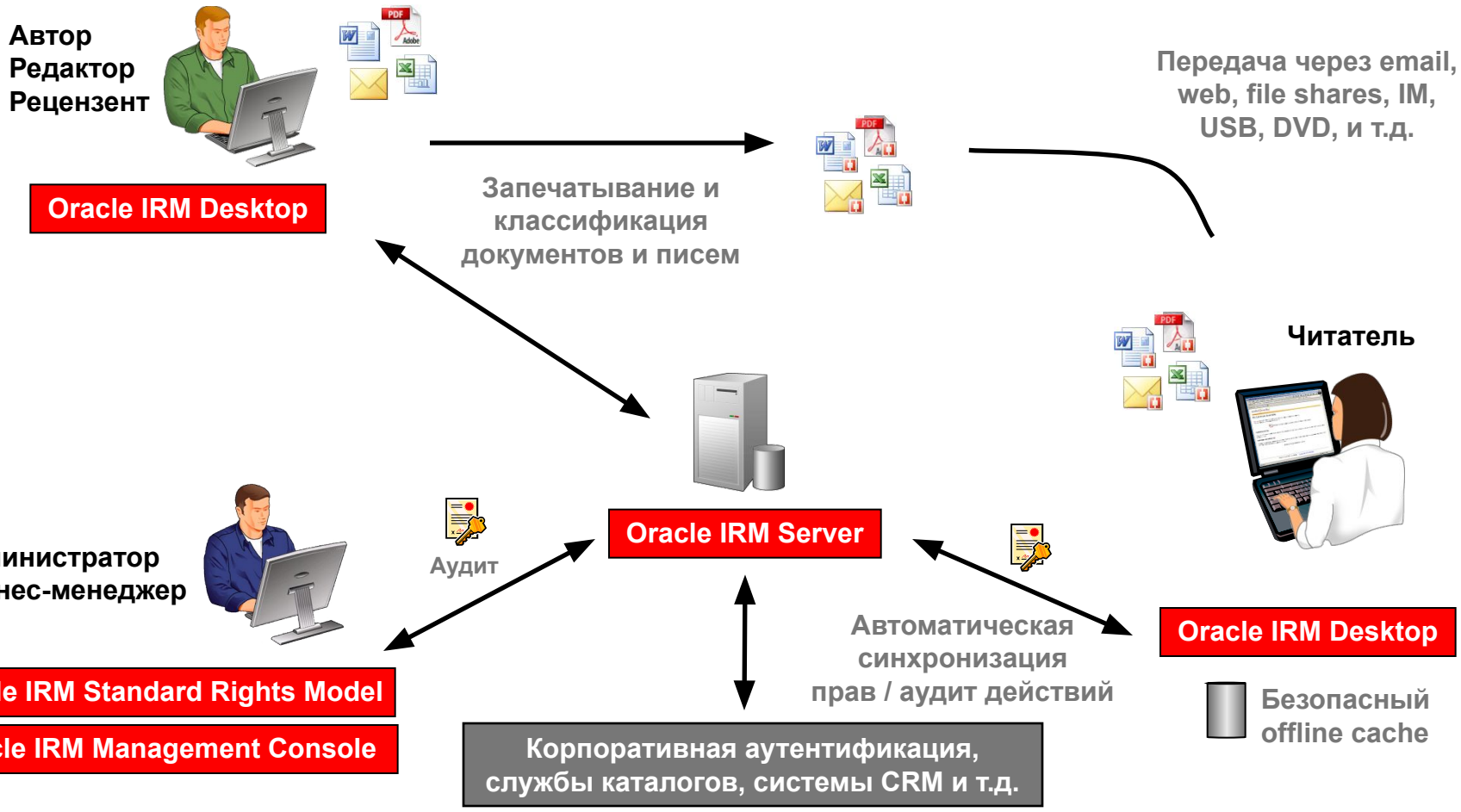


ORACLE

http://www.oracle.com/us/corporate/analystreports/infrastructure/index.html

# Защита документов с помощью Oracle Information Rights Management

## Управление классификацией, правами и аудитом






ORACLE

# Что позволяет сделать Oracle IRM

- Исключить неавторизованный доступ к защищаемым документам и всем их копиям; причем управление и контроль не останавливаются на межсетевом экране
- Применять ролевую авторизацию пользователей на выполнение предопределенного набора действий в документе
- Централизованно регистрировать использование документов и все попытки доступа; подготавливать соответствующие отчёты
- В любой момент централизованно изымать доступ ко всем копиям документа
- Управлять использованием версий документа

# Проблемы построения универсального решения

- Биллинг/АБС – имеет разные интерфейсы, в том числе и web, пользователи – в СУБД
- ERP/HRMS – имеет web интерфейс, хранит пользователей в СУБД/файле
- Система документооборота – некоторые модули имеют web интерфейс, хранит пользователей у себя, но может и в AD
- Service Desk – имеет web интерфейс, хранит пользователей у себя, но может и в AD
- Электронная почта – имеет свой интерфейс, пользователи в AD

**Требование минимального вмешательства в работу бизнес-систем диктует необходимость использования нескольких специализированных надсистемных решений по ИБ**

# Oracle Identity Management

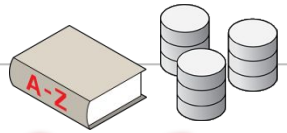
## Полнофункциональное первоклассное решение

### Администрирование учетных данных

- Доставка учетных данных с учетом ролевой модели
- Самообслуживание, заявки и подтверждения
- Управление паролями

### Управление доступом

- Аутентификация и борьба с мошенничеством
- Single Sign-On и федеративное взаимодействие
- Управление полномочиями и авторизация
- Безопасность Web-сервисов
- Защита электронных документов




### Службы каталогов

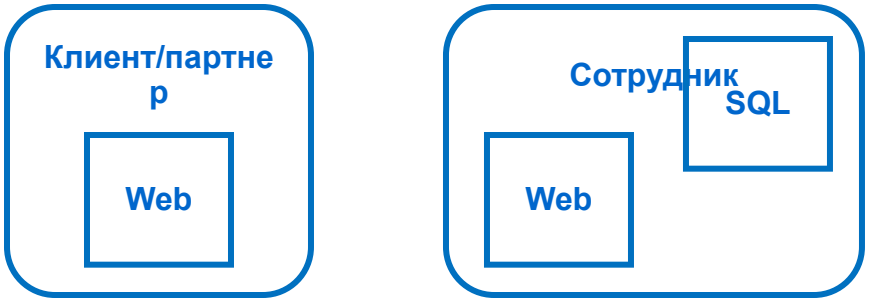
- LDAP-хранилища и их синхронизация
- Виртуализация хранилищ идентификационных данных

### Оптимизация учетных данных

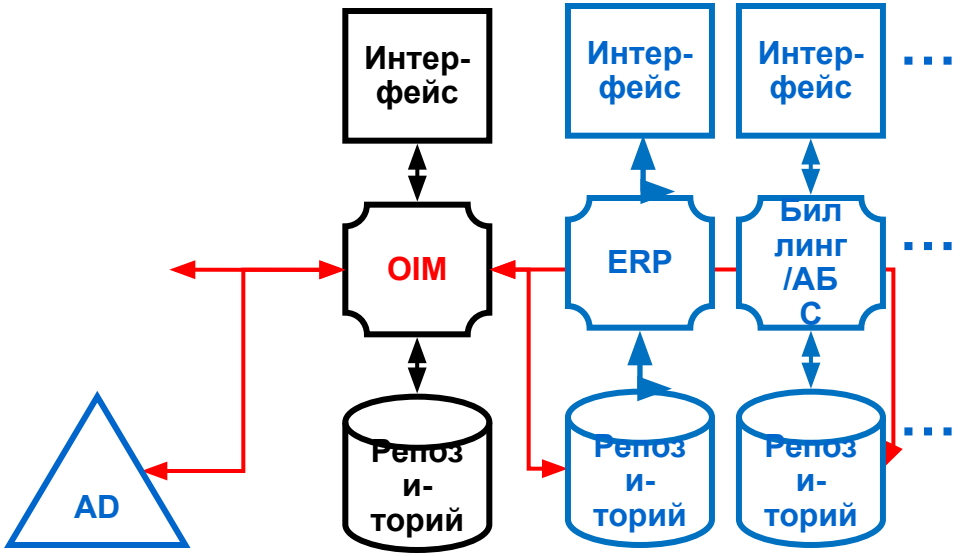
Аналитика, Разделение обязанностей, Ресертификация ролей и прав доступа

### Безопасность платформы

Идентификационные сервисы для разработчиков




# От встроенных в приложения средств защиты к централизованному управлению IT-привилегиями и контролю доступа



# Oracle Identity Manager через коннекторы позволяет автоматизировать процессы

- Создания учетных записей пользователей
- Выявления «сиротских» учетных записей
- Назначения / отзыва / изменения привилегий
- Разделения / делегирования полномочий
- Вовлечения в документооборот по изменению привилегий всех заинтересованных лиц с формализацией бизнес-процессов
- Контроля действий администраторов целевых систем
- Самообслуживания пользователей
  - Саморегистрация; заявки; смена / синхронизация паролей
- Ведения отчетности (оперативной / исторической)
- Временной блокировки / аттестации пользователей
- Удаления учетных записей пользователей

# Развертывание OIM

ОТДЕЛ КАДРОВ

ORACLE IDENTITY MANAGER

глобальные учетные записи OIM

членство

РОЛИ В ОРГАНИЗАЦИИ (ГЛОБАЛЬНЫЕ ГРУППЫ)

ГЛОБАЛЬНЫЕ ПОЛИТИКИ

ПОЛИТИКИ ДОСТУПА К ORACLE DB

создание учетных записей

привязка к ролям

членство

роль Oracle

ОБРАЗ РЕСУРСА ORACLE DB

ПОЛИТИКИ ДОСТУПА К MS AD

создание учетных записей

привязка к группам

членство

группа AD

ОБРАЗ РЕСУРСА MS AD

ПОЛИТИКИ ДОСТУПА К eBS

создание учетных записей

привязка к полномочиям

членство

полномочия

ОБРАЗ РЕСУРСА eBS

ЦЕЛЕВЫЕ СИСТЕМЫ

создание учетных записей

привязка к ролям

информация о ролях

роль Oracle

членство

учетные записи Oracle dB

права доступа

ресурс

создание учетных записей

привязка к группам

информация о группах

группа AD

членство

учетные записи MS AD

права доступа

ресурс

создание учетных записей

привязка к полномочиям

информация о полномочиях

полномочия

членство

учетные записи eBS

права доступа

ресурс

# Преимущества использования OIM

## Управление жизненным циклом учетных записей

**Усиление безопасности IT-инфраструктуры**

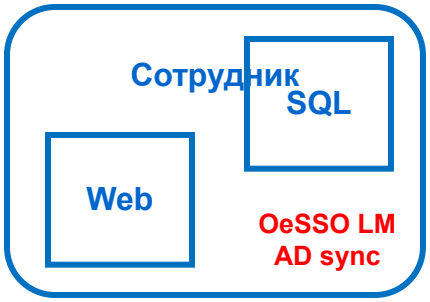
- Единое решение для управления пользовательскими привилегиями в различных системах
- Исключение фрагментации пользовательских профилей между хранилищами в таблицах, базах данных, каталогах
- Формализация IT-привилегий и их привязка к бизнес-ролям
- Достоверные данные аудита прав и истории принятия решений

**Снижение расходов**

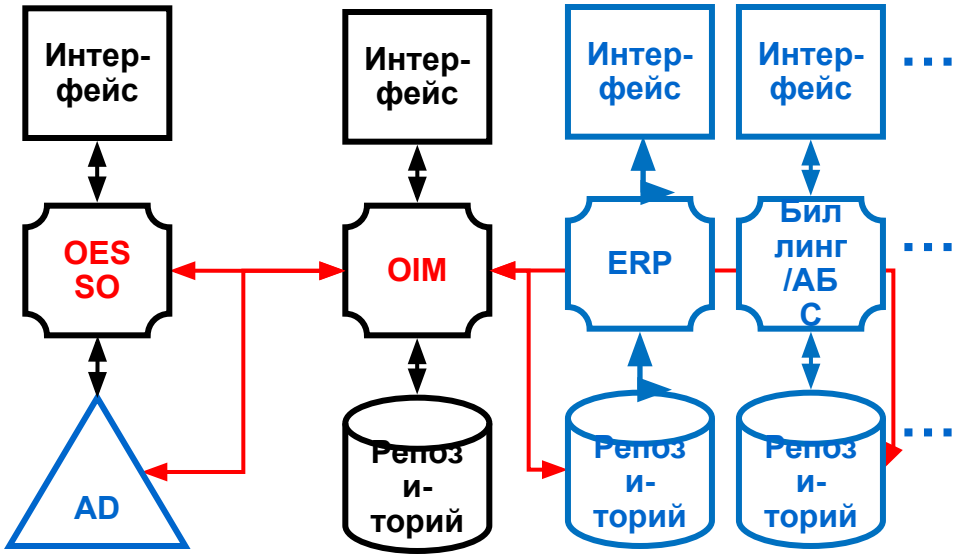
- Самообслуживание пользователей
- Аттестация, согласование заявок

**Упрощение внедрения и интеграции**

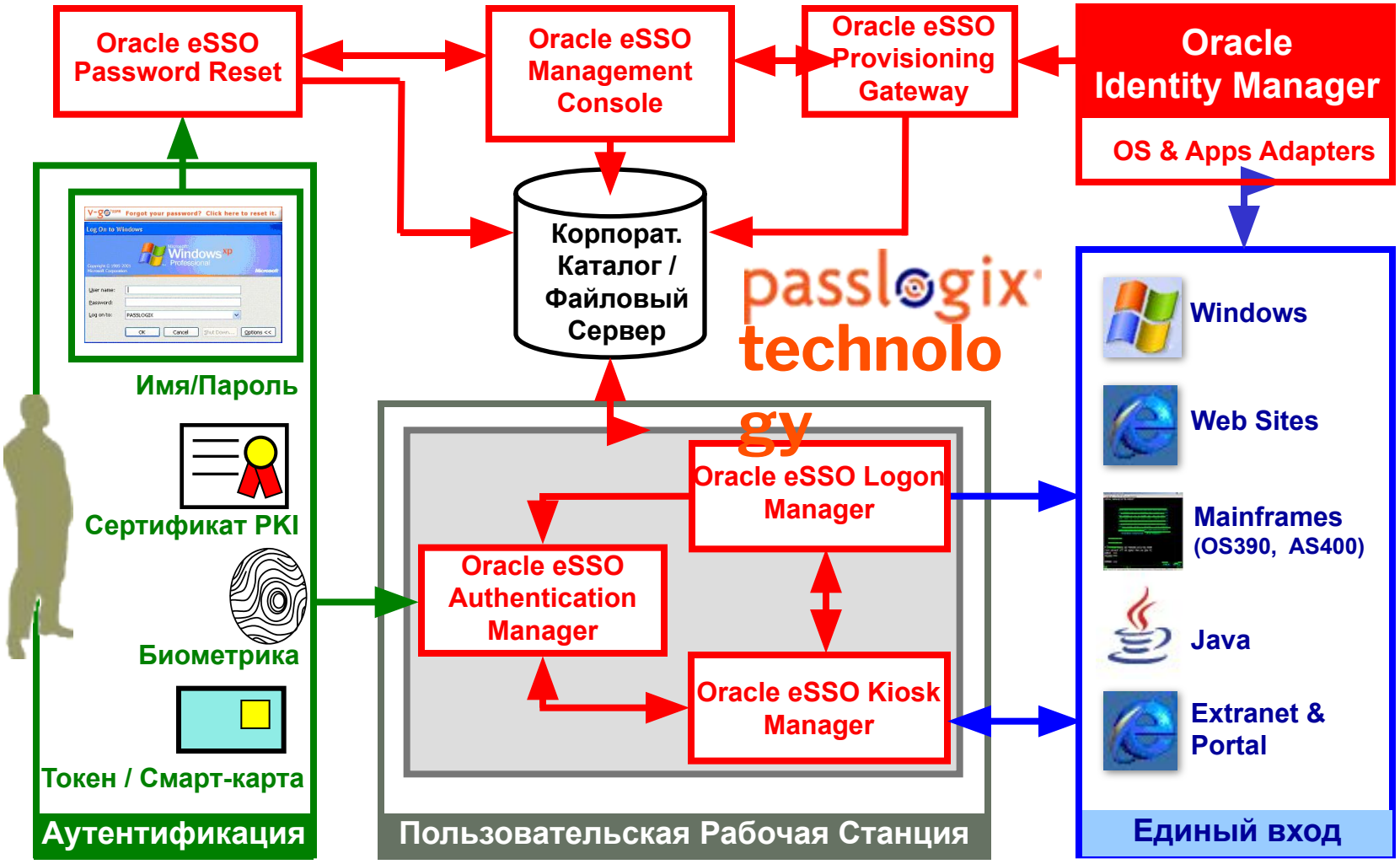
- С централизованными системами контроля доступа (включая OAM, OeSSO, доступ к помещениям, управление токенами и т.п.)


# От встроенных в приложения средств защиты к централизованному управлению IT-привилегиями и контролю доступа



# Передача приложениям ID-данных с помощью Oracle Enterprise SSO Suite



# Преимущества использования ESSO

## Прозрачное подключение к унаследованным приложениям

**Усиление безопасности IT-инфраструктуры**

- Возможность усиления аутентификации для унаследованных приложений
- Аудит подключений пользователей к приложениям

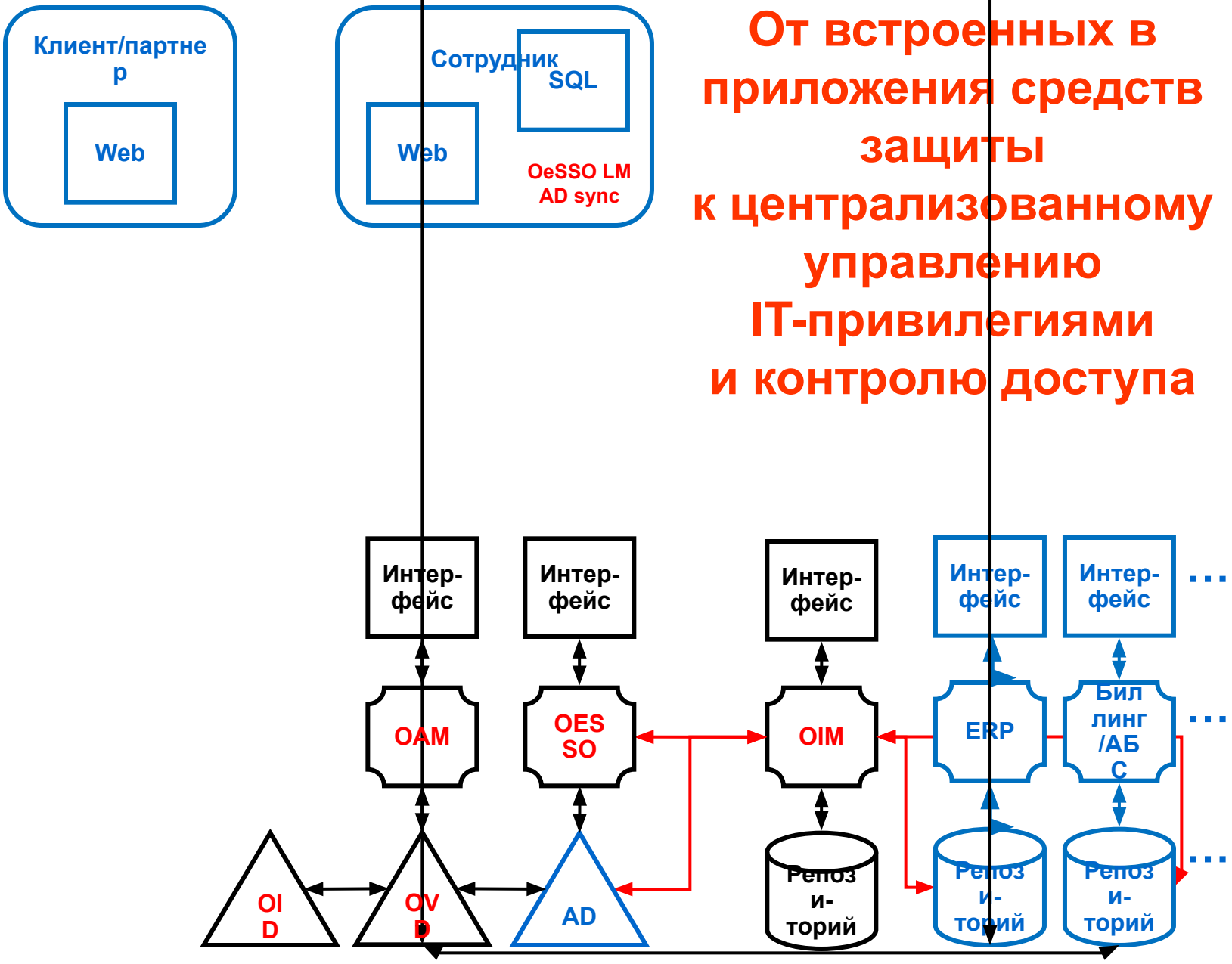
**Повышение степени удовлетворенности сотрудников**

- Легкий доступ пользователей к множеству корпоративных приложений с помощью единственного пароля
- Легкая смена паролей с подсказками для проверки правил сложности
- Возможность сброса пароля в MS AD, даже если он забыт

**Упрощение внедрения и интеграции**

- Интеграция с аппаратными аутентификаторами
- Интеграция с системой доставки идентификационных данных

# От встроенных в приложения средств защиты к централизованному управлению IT-привилегиями и контролю доступа



# Контроль доступа к Web-приложениям и SSO с помощью Oracle Access Manager

http://www.autoparts.com/credit-check


**Централизо-ванные AAA:**

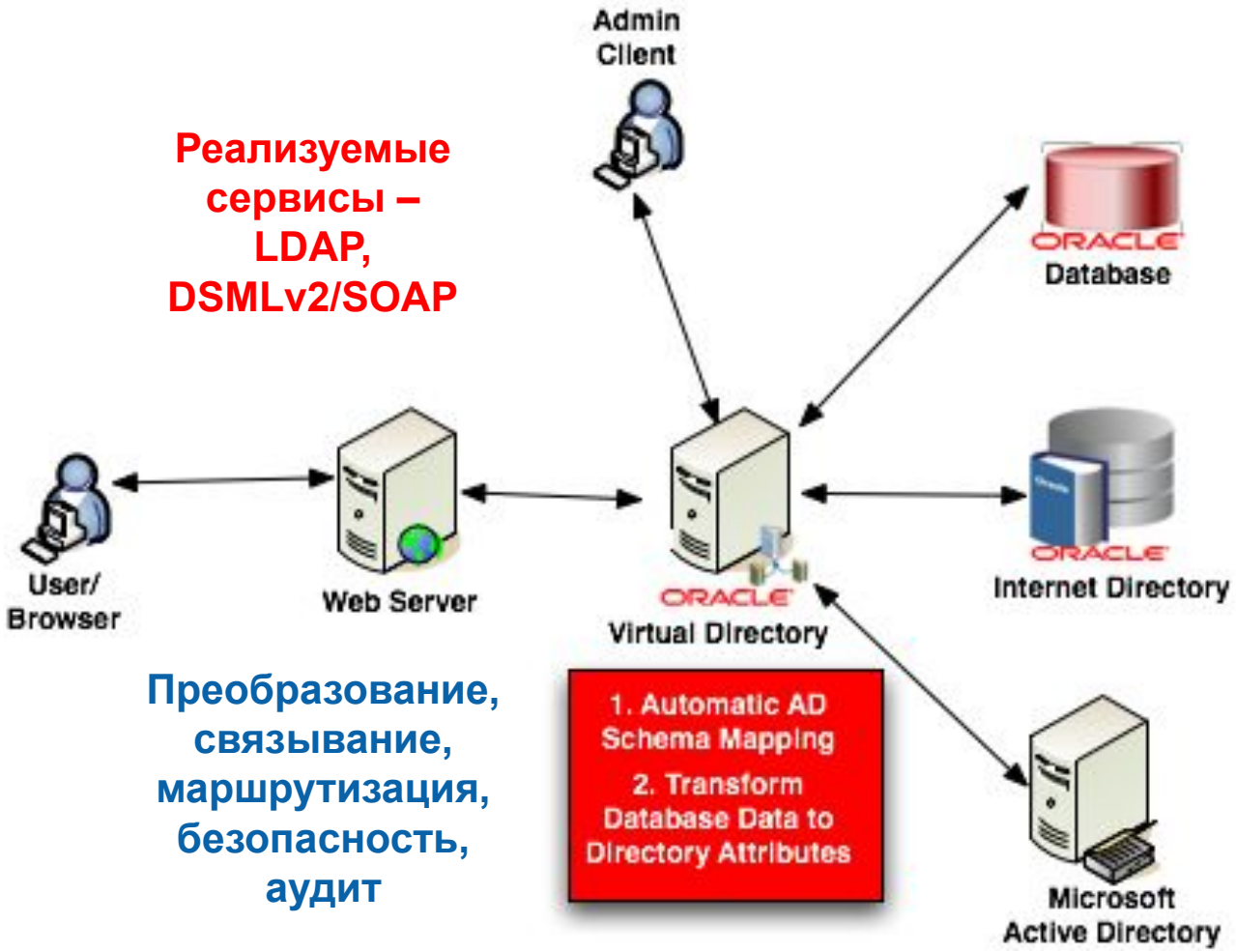
- Аутенти-фикация
- Авторизация
- Аудит

- Страница защищена?
- Вы аутентифицированы?
- Доступ разрешен?

LDAP

**Клиент** | **Шлюз** | **Сервер управления доступом** | **Каталог** | **Информационный ресурс**

# «Распределенная консолидация» учетных данных в Oracle Virtual Directory



# Преимущества использования OVD

## Консолидация учетных данных без их синхронизации

**Консолидация разрозненных идентификационных данных**

- Быстрая реализация проекта
- Схема данных в хранилищах не меняется
- Возможно создание корпоративного справочника

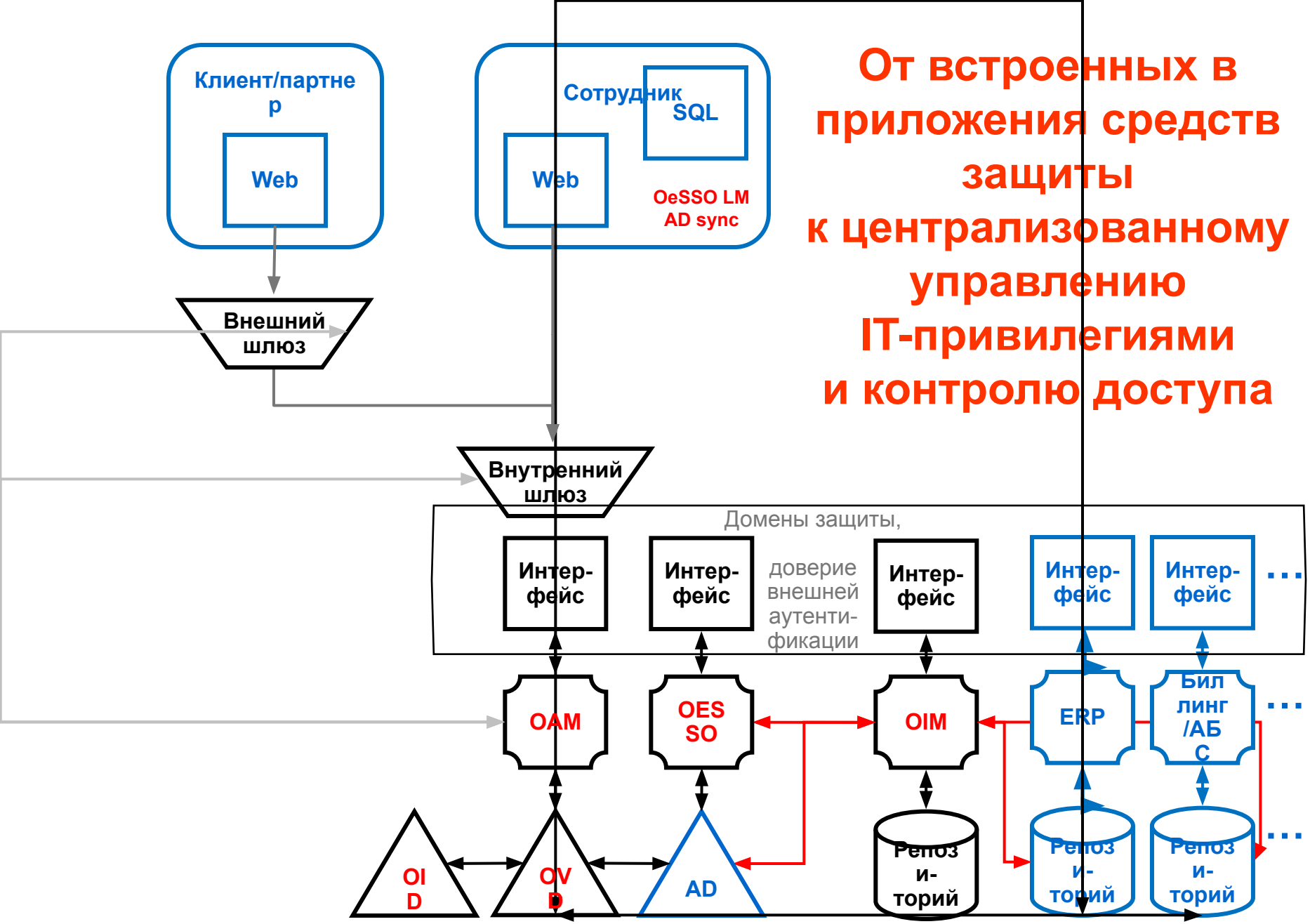
**Усиление безопасности IT-инфраструктуры**

- Защита хранилищ идентификационных данных за счет их сокрытия
- Снятие нагрузки с каталогов за счет кэширования, отказоустойчивость

**Упрощение внедрения и интеграции**

- Решение позволяет снять ограничения на структуру идентификационных данных при внедрении портальных решений (например, преобразовать доменный «лес» в «ветку»)

# От встроенных в приложения средств защиты к централизованному управлению IT-привилегиями и контролю доступа



# Преимущества использования OAM

## Управление доступом к Web-приложениям

**Повышение степени удовлетворенности сотрудников, партнеров и заказчиков**

- Легкий доступ пользователей к множеству Web-приложений с однократной регистрацией
- Возможность аутентификации по ГОСТовым сертификатам

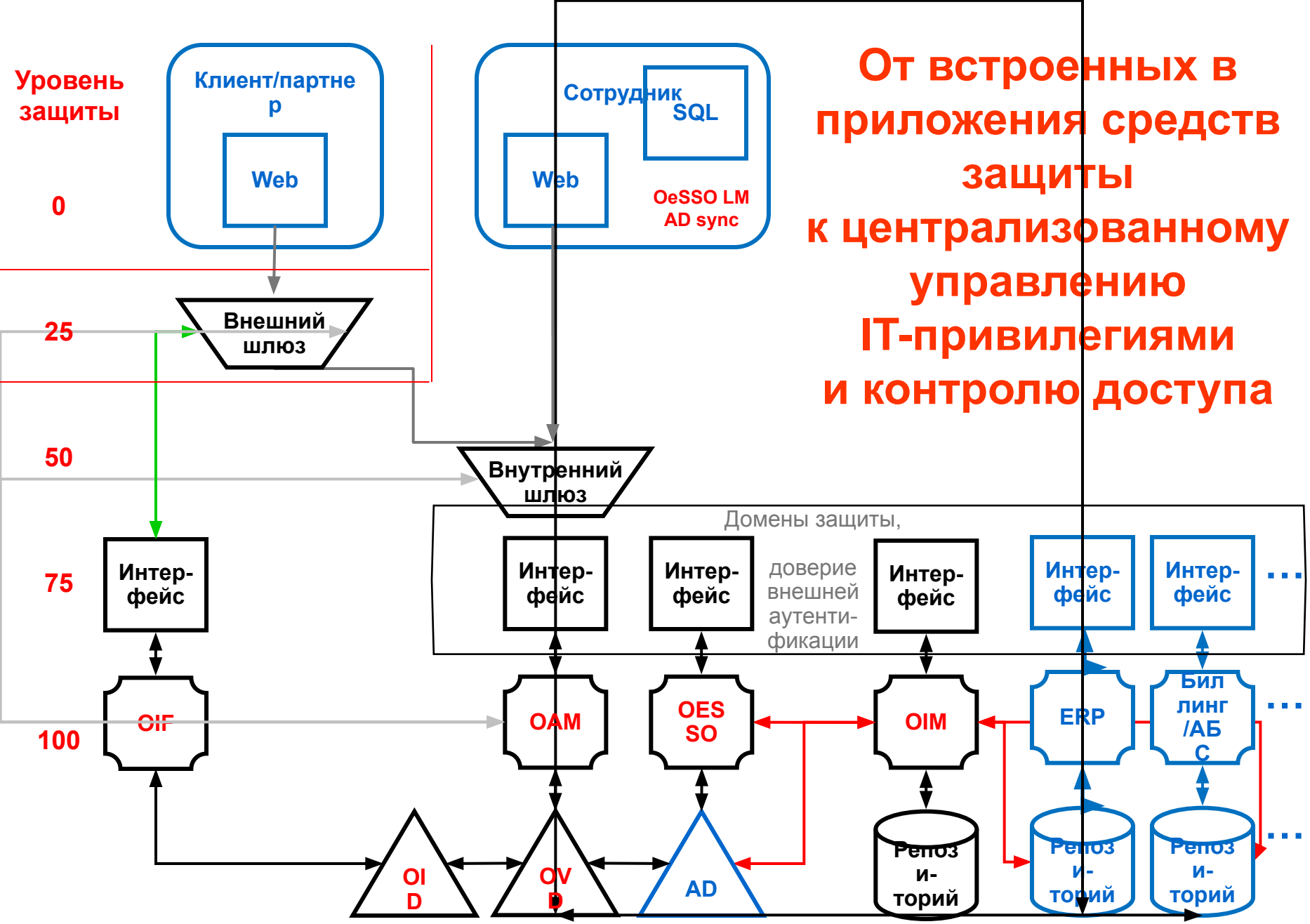
**Повышение степени защищенности приложений**

- Единые политики доступа, включая
  - Усиленную аутентификацию
  - Авторизацию по ACL, политикам и бизнес-логике
  - Аудит доступа
- Отказоустойчивость и масштабируемость системы

**Упрощение внедрения и интеграции**

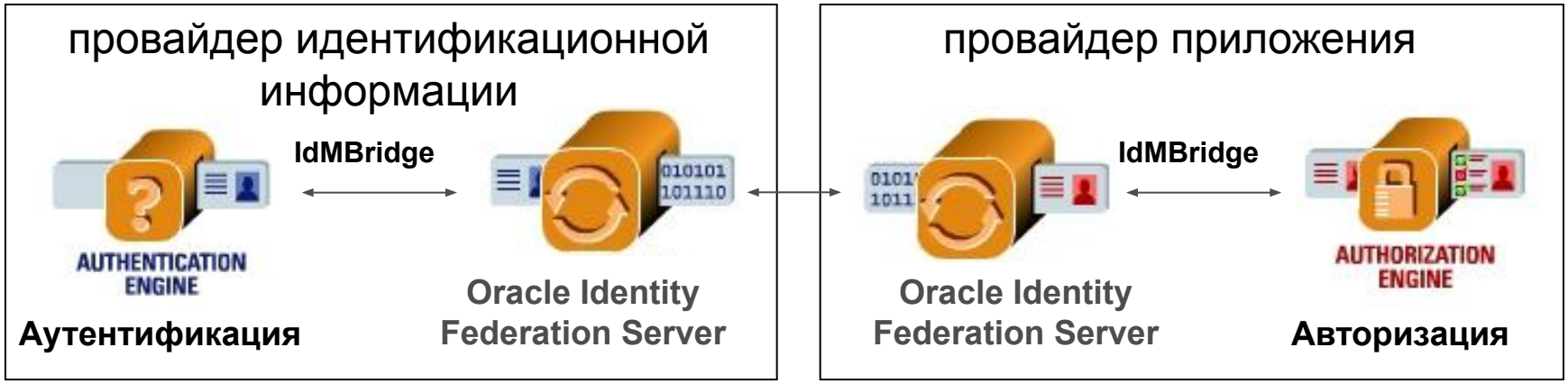
- Повторное использование сервера управления доступом при добавлении новых приложений или сервисов

# От встроенных в приложения средств защиты к централизованному управлению IT-привилегиями и контролю доступа

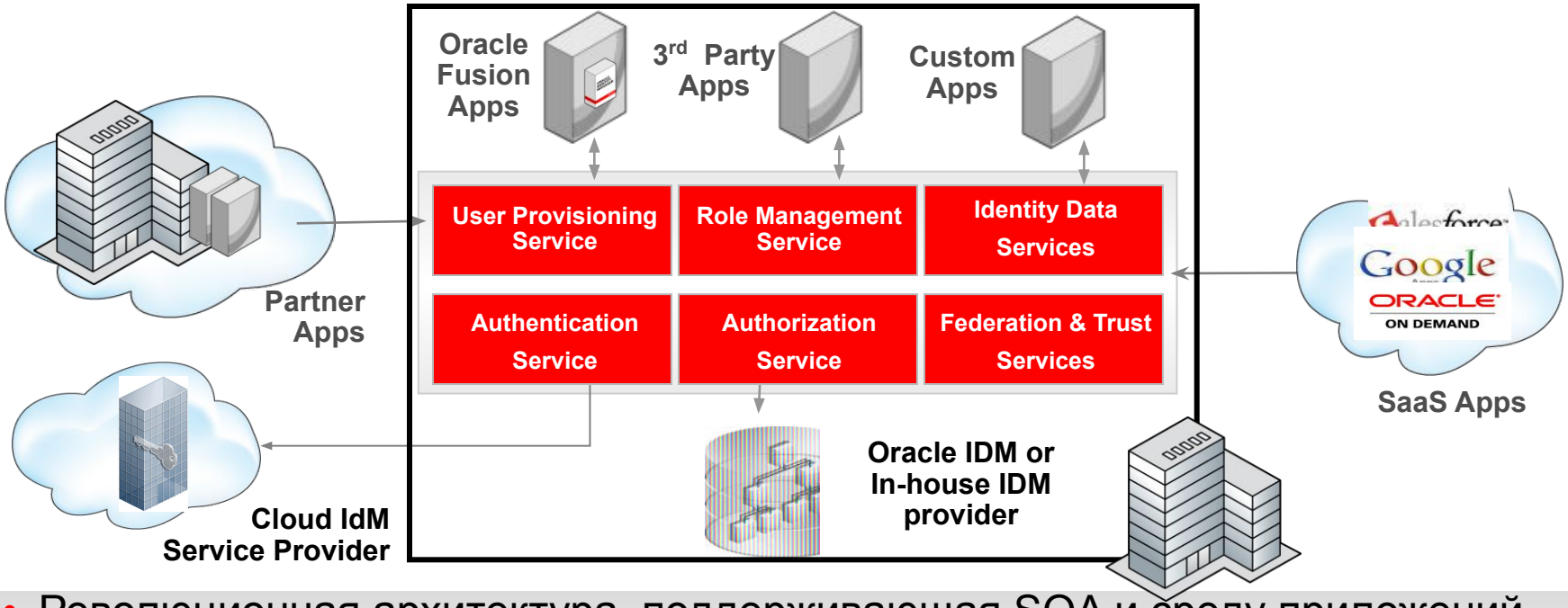


# Oracle Identity Federation – WebSSO для пользователей филиалов и партнеров

- После успешной аутентификации у провайдера IDs пользователь обращается к защищенному внешнему ресурсу
- OIF сервер провайдера IDs создает подтверждение (assertion) SAML, основываясь на профиле провайдера приложения
- OIF сервер провайдера приложения получает подтверждение  и соотносит внешнего пользователя с локальным, проверяет его права доступа к запрошенному ресурсу и, при положительной авторизации, перенаправляет браузер пользователя к своему приложению.



# Oracle Identity Management реализует модель «Безопасность как Сервис»




- Революционная архитектура, поддерживающая SOA и среду приложений
- Целостные, повторно используемые сервисы безопасности
- Возможность подключения внешних сервисов (включая облачные Identity Services) в дополнение к собственным
- Легкое подключение, обеспечивающее долговременную устойчивость и гетерогенность бизнес-решений

# Мнение аналитиков: Oracle – №1 в IdM

FORRESTER®

**Figure 2** Forrester Wave™: Identity And Access Management, Q4 '09

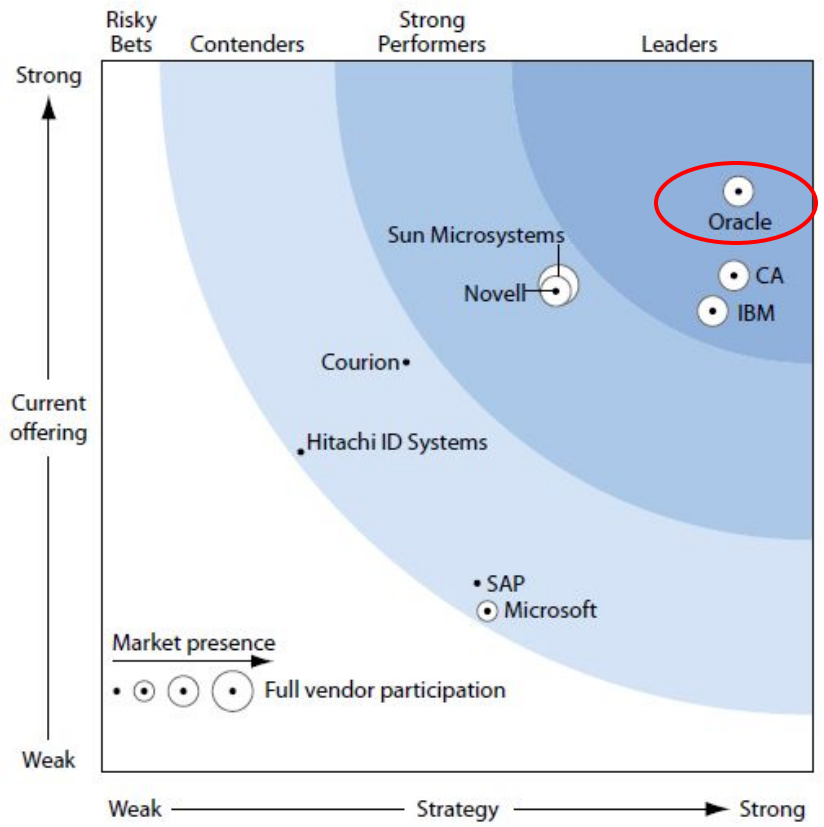
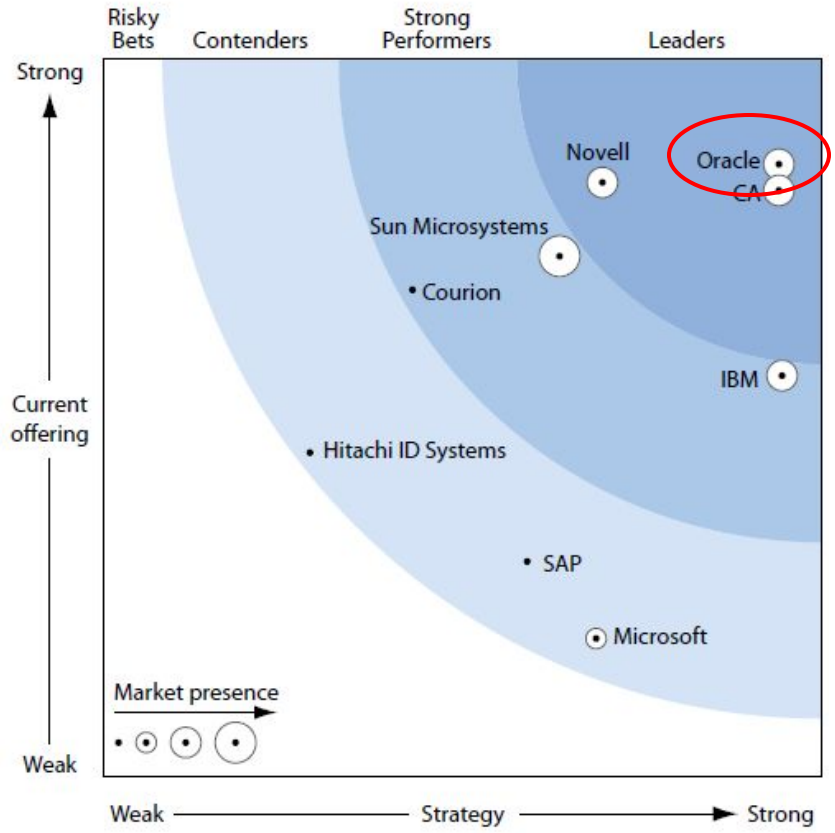



**Figure 3** Forrester Wave™: Provisioning, Q4 '09





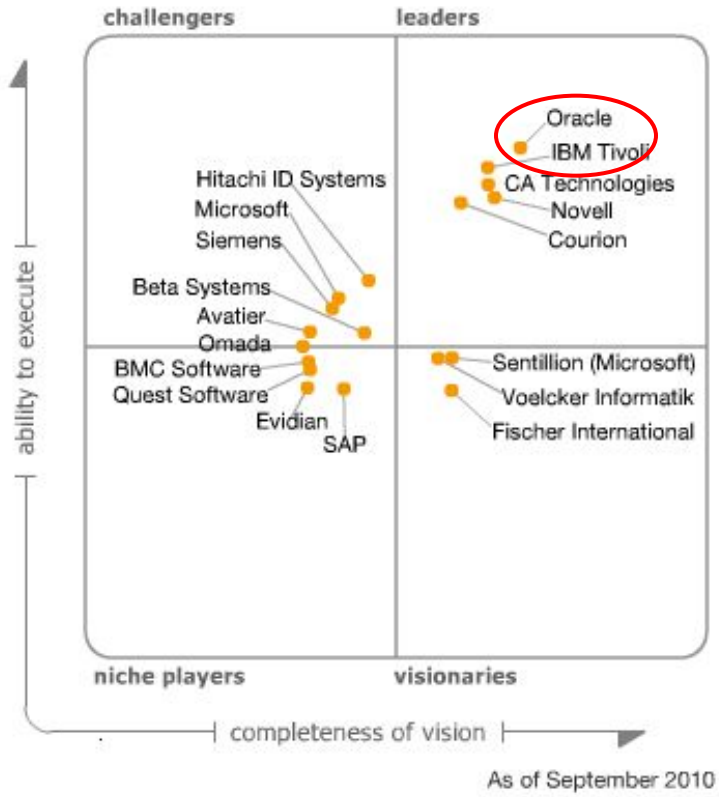

ORACLE

http://www.oracle.com/us/corporate/analystreports/infrastructure/059631.pdf

# Oracle - лидер рынка в областях доставки учетных данных и управления доступом

## Gartner's Magic Quadrants

### User Provisioning, 2H 2010




### Web Access Management, 2H 2009

# Решение недавно приобретенной компании Passlogix также считается лучшим

## Gartner's Magic Quadrants for Enterprise Single Sign-On, 2H 2008




ORACLE

# С чем Oracle идет к заказчикам в России

**Решения Oracle в области информационной безопасности**

**=**

**Технологии мирового уровня**

**+**

**Знание и учет национальной специфики**

Опора на партнеров, обладающих полномочиями по выполнению работ, связанных с обеспечением информационной безопасности

- Системные интеграторы
- Компании-разработчики программного обеспечения
- Центры компетенции по информационной безопасности

# Референсные заказчики и ключевые партнеры в России

- ПромСвязьБанк http://oracleday.ru/agenda.html – Fors
- СУЭК http://www.ibs.ru/content/rus/545/5453-article.asp – IBS Borlas
- ПетроКоммерц, Иркут http://www.jet.msk.su/press_center/news/archive_of_news/detail.php?ID=3075 – Jet Infosystems
- ВТБ http://rdtex.ru/win/root/news_all.html – RDTEX + Lins-M
- Аэрофлот http://www.pcweek.ru/themes/detail.php?ID=104989, Университет ФизКультуры Спорта и Туризма http://www.r-style.ru/presscenter/news/oracle_IAMS/, СИБУР http://www.r-style.ru/presscenter/news/sibur-ident/ – R-Style
- Опытные партнеры
  - Croc, RNT, Elvis+, ICL
  - Астерос, Sitronics, Газинформсервис
  - ISV и интеграционные решения ЕВРААС.ИТ, InfoWatch

# Oracle Enterprise Security – ресурсы

- Блог «Информационная Безопасность - Решения Oracle» http://security-orcl.blogspot.com/
- Брошюра «Техническое описание Oracle Identity Management 11g» http://security-orcl.blogspot.com/2011/01/blog-post_14.html
- Библиотека документов на русском языке http://www.oracle.com/global/ru/pdfs/index.html
- Страница «Управление идентификационной информацией» http://www.oracle.com/ru/products/middleware/identity-management/index.html
- Библиотека документов на английском языке по IdM http://www.oracle.com/us/products/middleware/identity-management/resource-library/index.html
- Страница «Oracle Database Security and Compliance» http://www.oracle.com/technetwork/database/security/index.html

# Соответствие требованиям ФЗ РФ №152 затратно, но надо постараться получить дополнительную выгоду от решения!

Соответствие требованиям законодательства


Финансовая эффективность

# Устраняем преграды...

- Сертификация ФСТЭКом наших решений
  - Oracle DB + Oracle DB Vault
  - Oracle IAMS
  - Oracle ESSO
  - Oracle IRM
- Локализация
- Региональный маркетинг

Разные модели угроз

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

## СЕРТИФИКАТ СООТВЕТСТВИЯ
## № 2238

Выдан 23 декабря 2010 г.
Действителен до 23 декабря 2013 г.

Настоящий сертификат удостоверяет, что **программное обеспечение Oracle Identity Access Management Suite 11g** (партия из 200 (двухсот) экземпляров продукции с идентификационными №№ с 0001 по 0200, маркированных знаками соответствия с № Г 617000 по № Г 617199) производства компании Oracle, Inc. является программным средством, обеспечивающим разграничение доступа к информации, не содержащей сведения, составляющие государственную тайну, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по **4** уровню контроля и технических условий ТУ-5014-002-52384799-2007, и может использоваться при создании автоматизированных систем до класса защищенности **1Г** включительно, а также для защиты информации в информационных системах персональных данных до **1** класса включительно.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Главный испытательный сертификационный центр программных средств вычислительной техники» (аттестат аккредитации от 08.04.2010 № СЗИ RU.2503.Б91.069) - техническое заключение от 01.10.2010 и экспертного заключения от 09.12.2010 органа по сертификации ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.А92.007).

Заявитель: ООО «ФОРС-Центр разработки»
Адрес: 129272, г. Москва, Трифоновский тупик, д. 3
Телефон: (495) 787-7040

Маркирование знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям указанных в настоящем сертификате руководящего документа и технических условий осуществляется испытательной лабораторией ООО «Главный испытательный сертификационный центр программных средств вычислительной техники».

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Селин

# Программа сертификации решений

- Информация – в Государственном реестре сертифицированных средств защиты информации на Официальном сайте Федеральной службы по техническому и экспортному контролю на http://www.fstec.ru/_razd/_serto.htm

- Актуальные сертификаты
  - На СУБД Oracle с опцией DB Vault
    - Версии 11 на Windows 64 bit (#1849)
    - Версии 10 на RedHat, HPUX и Solaris (#2265)
  - На IAMS версии 10 (#1664) и 11 (#2238)
  - На IRM версии 10 (#1801) и 11 (#2128)
  - На ESSO версии 10 (#1802)

# Что изменится с внедрением IAMS

## Технологии

- Биллинг/АБС, ERP, Система документооборота
  - автоматизированное изменение и исторический контроль привилегий, заявки, согласования, выявление «сиротских» учетных записей, контроль неизбыточности полномочий
  - SSO, первичная авторизация и аудит обращений для Web-интерфейсов
- Биллинг/HRMS
  - еще и виртуальный профиль пользователя
- Service Desk
  - еще и виртуальный справочник
- Электронная почта
  - SSO для Web-интерфейса

# Что изменится с внедрением IAMS

## Возврат инвестиций

- Снижение рисков (DLP, Compliance)
- Ускорение бизнес-процессов
  - Назначения, изменения, отзыва IT-привилегий
  - Подготовки отчетности
  - Подключения новых систем
- Снижение нагрузки на help-desk
  - Консолидированные данные
  - Самообслуживание пользователей
- Косвенные факторы
  - Повышение качества обслуживания (возможность SLA)
  - Оптимизация ролевой модели и пула лицензий

# Ожидаемые финансовые результаты

## По данным Radicati Group и экспертным оценкам

- Снижение TCO
- Сокращение связанного с IdM простоя сотрудников на 78%
- Сокращения затрат на ИТ-аудит на 75%
- Снижение лицензионных отчислений для бизнес-приложений до 30%
- Снижение рисков информационной безопасности на 15%
- Повышение производительности Help Desk на 55%
- Повышение эффективности управления учетными записями на 78%
- Финансовая эффективность
- ROI- 60-70%, окупаемость 2-3 года

# Вопросы

123317, Россия, Москва, Пресненская набережная, 10
Башня на Набережной, Блок С
(+7495) 6411400 Andrey.Gusakov@Oracle.Com

# Концепция IT-безопасности и определение конфиденциальности

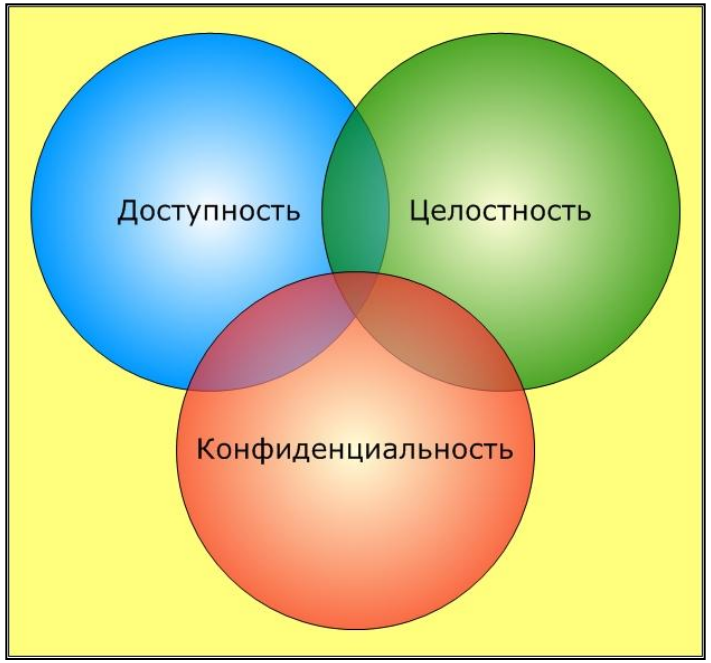
«Критичные данные должны быть доступны только уполномоченным лицам только тем способом, который разрешён политикой безопасности и только с помощью средств определенных политикой безопасности»

(классификация)

(управление IT-привилегиями)

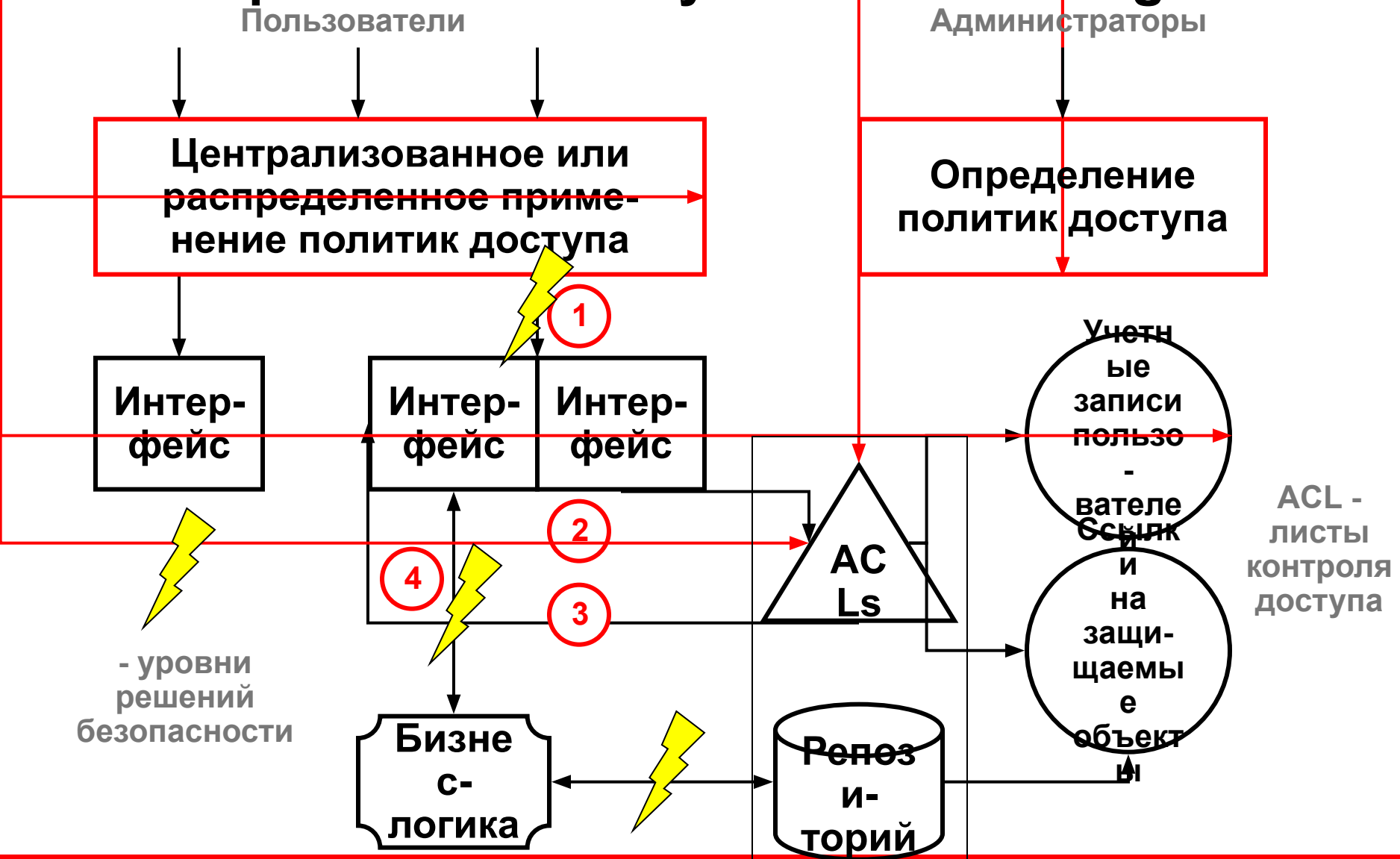
(аудит)

(управление доступом)




-> единая стратегия

# Как работает Identity & Access Management



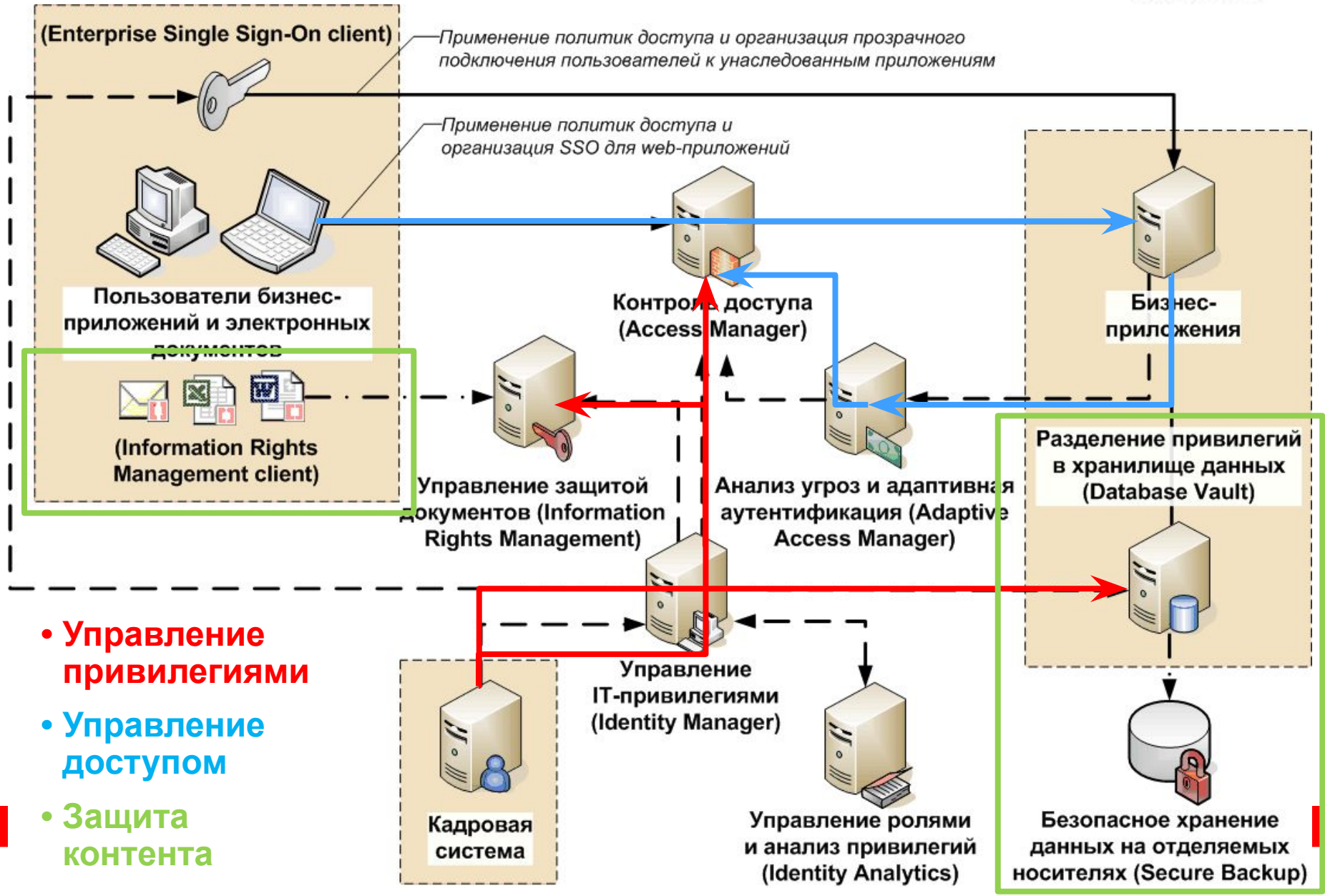



ORACLE

Управление Доступом (Web & Enterprise SSO)

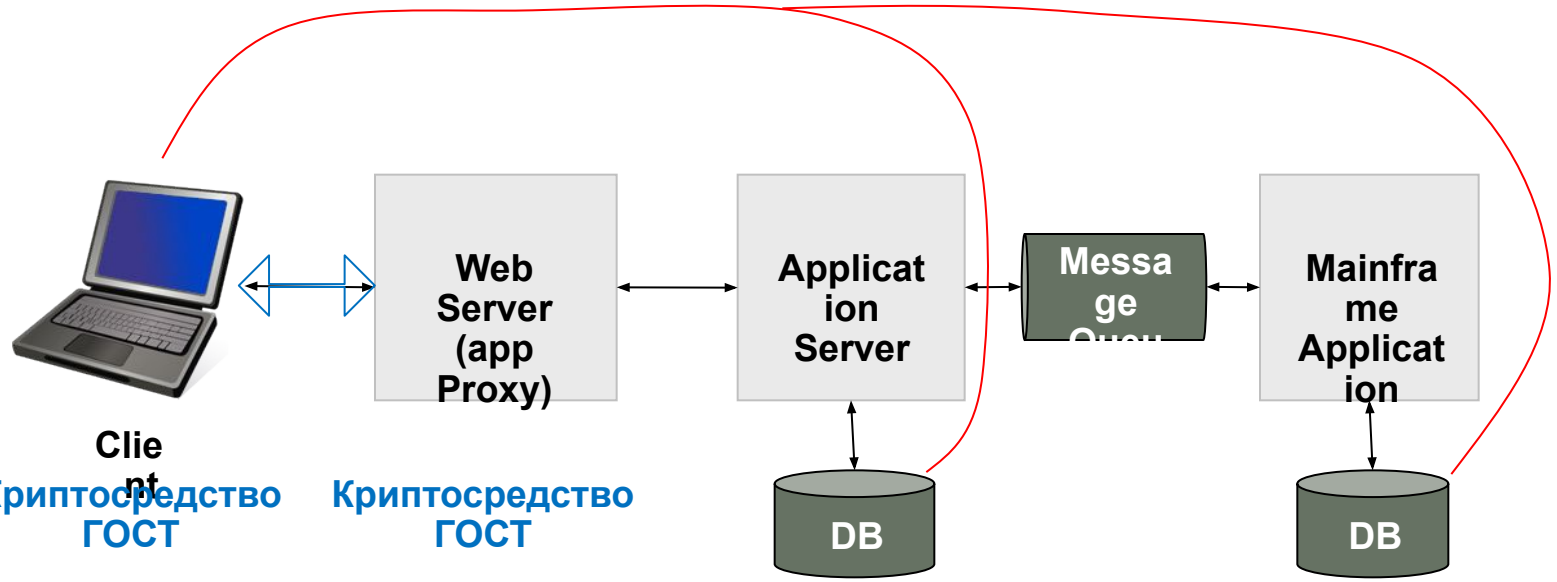
Управление Привилегиями (Reconciliation & Provisioning)

# Автоматизация бизнес-процессов с ORACLE SECURITY




- **Управление привилегиями**
- **Управление доступом**
- **Защита контента**

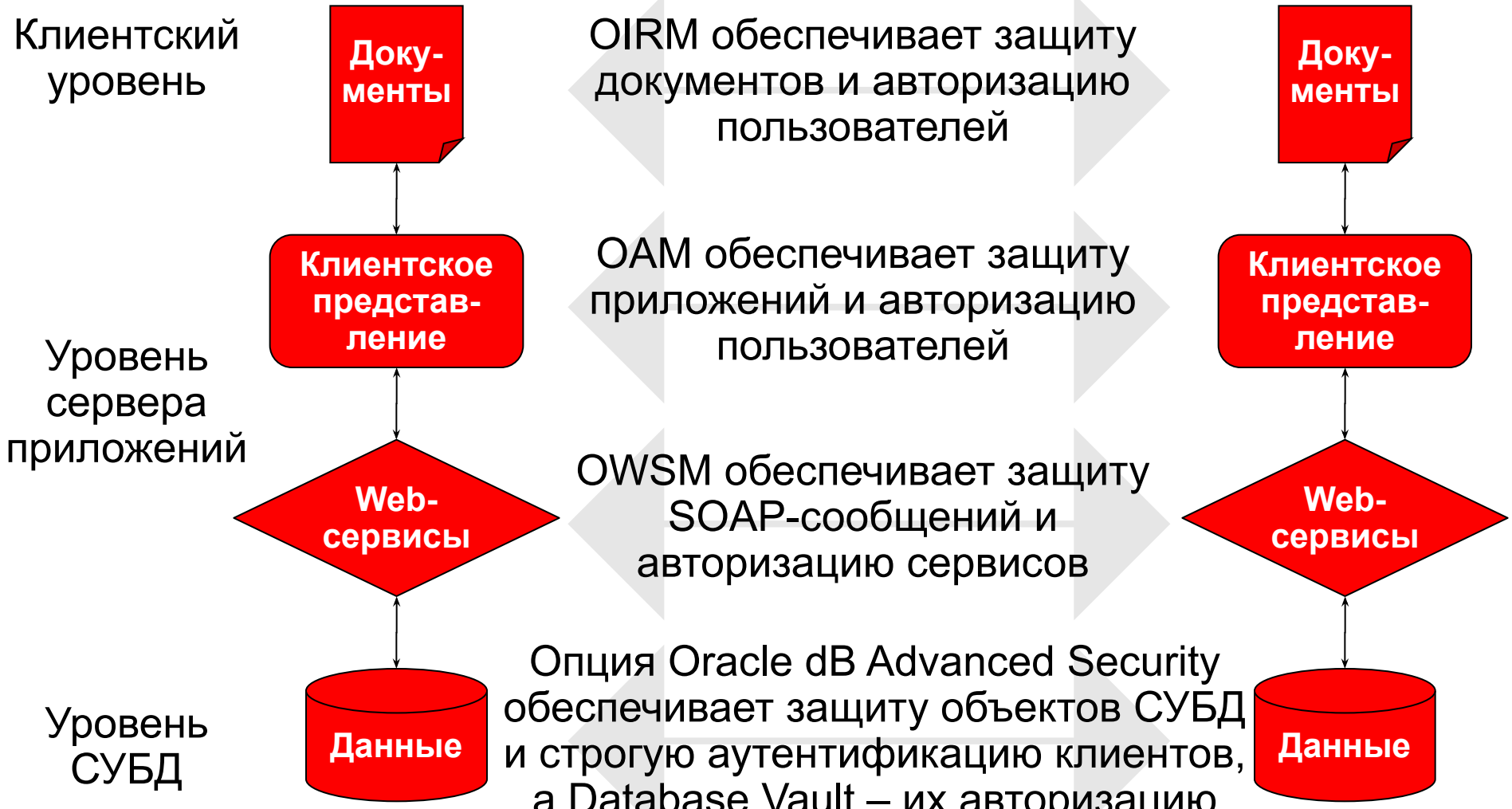
# Достаточно ли защиты каналов для обеспечения целостности информации?



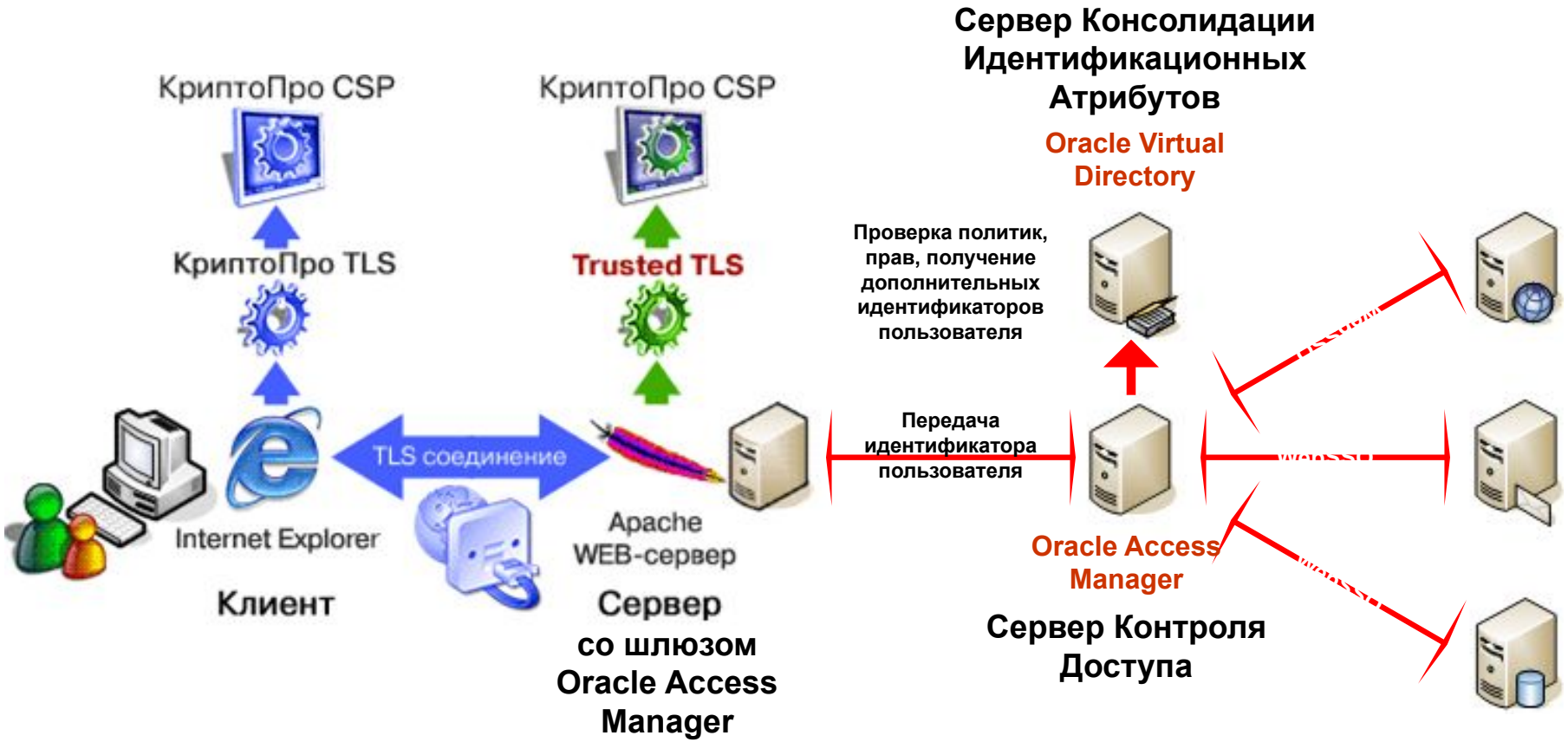

Нежелательность раскрытия информации на хостах требует защиты самих сообщений

В SOA-среде эту роль выполняет Oracle Web Services Manager

# Защита информации при ее передаче



# Использование сертифицированных криптоалгоритмов для WebSSO




Подробности – на нашем блоге http://security-orcl.blogspot.com/

# Перспективы Oracle Identity Manager в России и мире