



**Практическая безопасность в
банках**

**EXTREME
PERFORMANCE**

ORACLE®

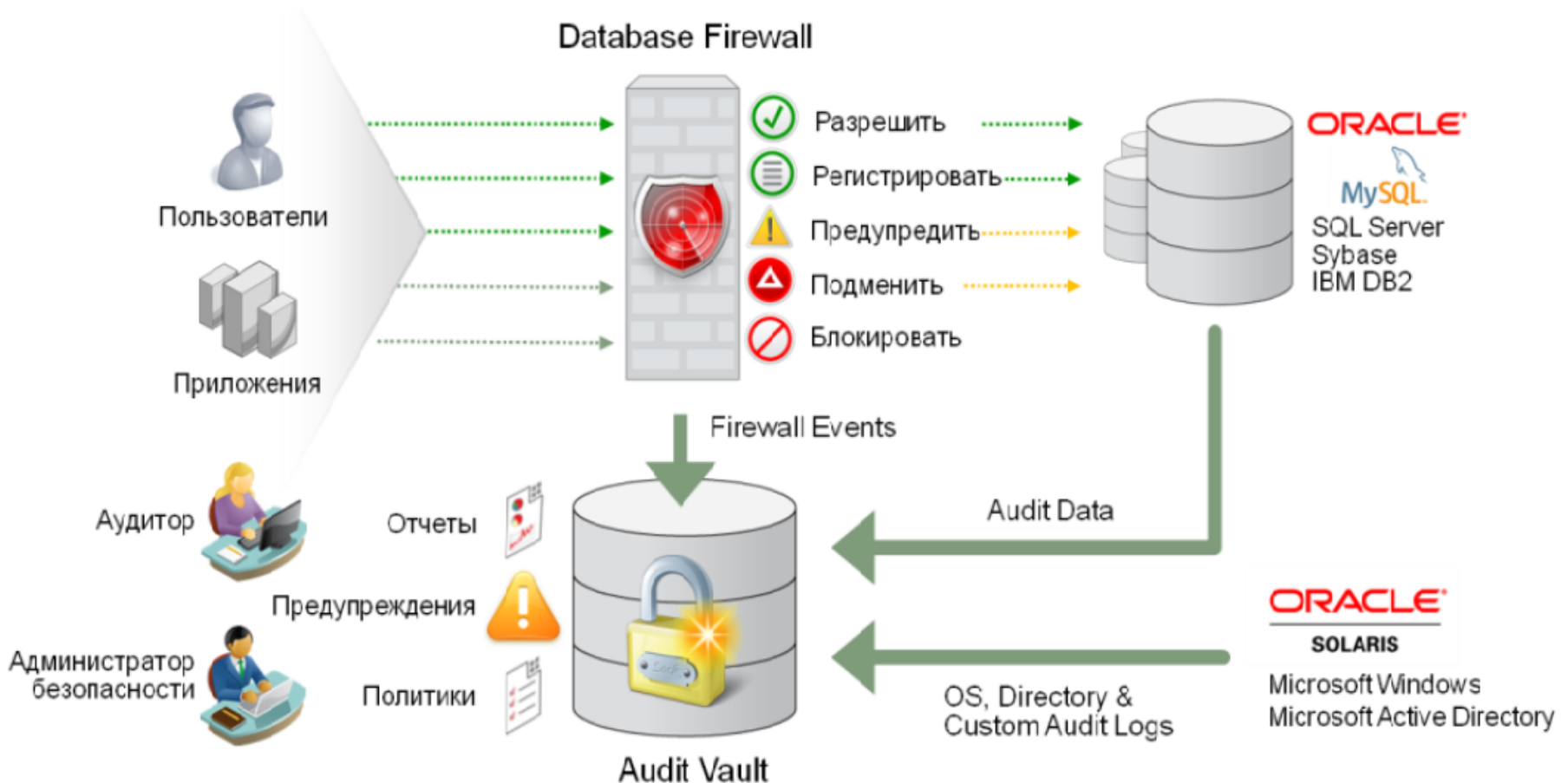
**Руслан Бялькин
Директор по работе с ключевыми
клиентами**

Решения для защиты информации

- **Database Security**
- **Oracle Identity and Access Management Suite**
- **WebCenter Content**
- **Oracle Sun Ray**
- **Oracle Enterprise GRCM**

Первая линия защиты

Oracle Audit Vault and Database Firewall



Комплексная защита хранилища данных на примере системы ДБО

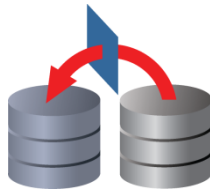
Сервер приложений системы ДБО

‘Клон’

базы данных

Имя	N. Полиса	Зарплата
LJON	111-56-9876	125,000
TDPQQ	111-76-1234	229,500
TNJQI	111-78-2198	53,700

Обезличивание данных для систем тестирования и разработок
Data Masking Pack



Защита и шифрование передаваемых данных
Advanced Security Option



Контроль доступа к данным
Database Vault

Database Vault	Администратор БД	Пользователь
Select SALARY from users;	X	✓
Alter system. Alter table..	✓	X

* Пример ролей и полномочий

Удаление персональных данных и конфиденциальных сведений

Защита и шифрование данных, хранящихся в БД
Advanced Security Option



Alter table ...



Администратор БД

Select SALARY from USERS;

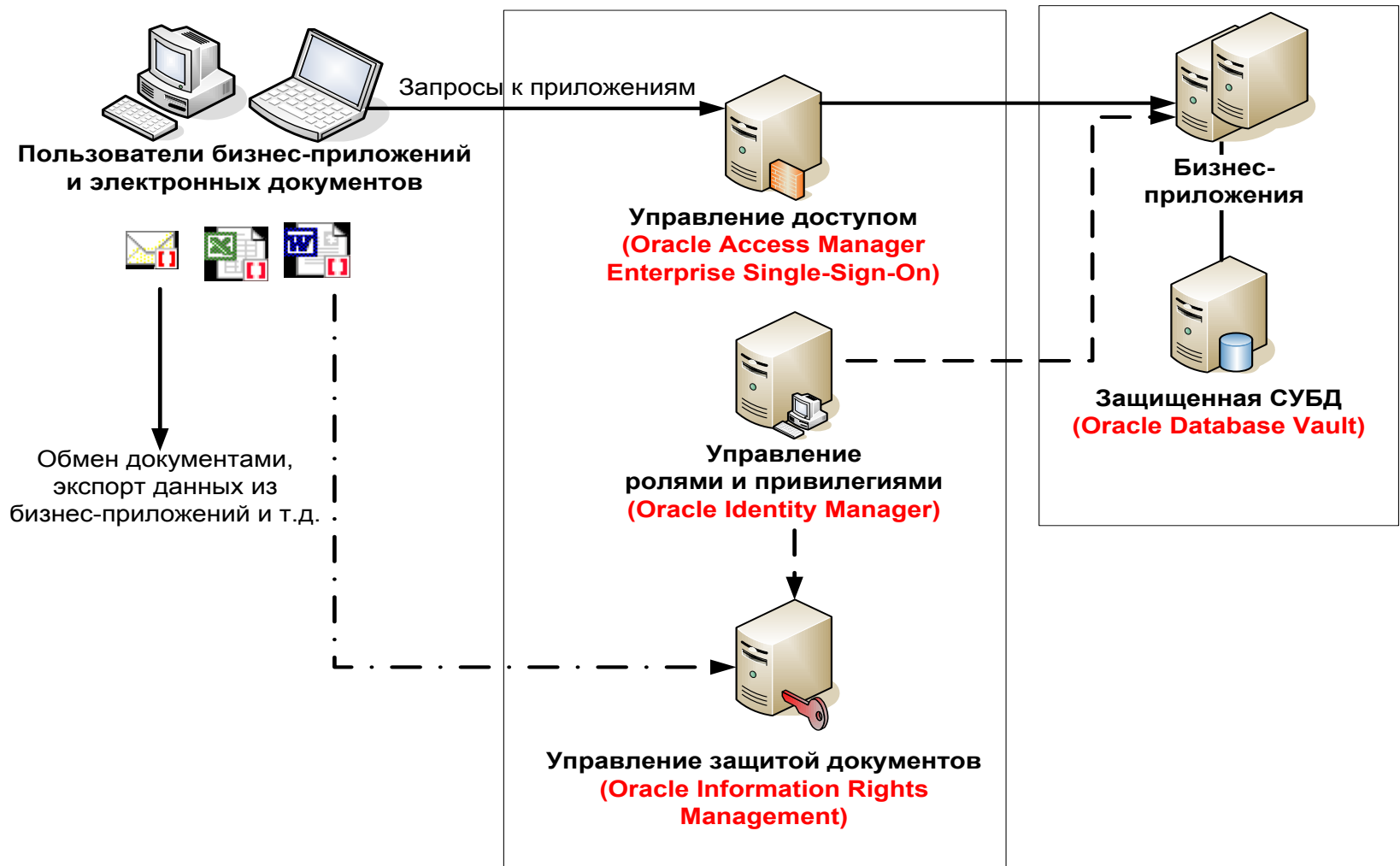


БД, содержащая сведения о доступе к БД
Audit Vault

Имя	N. полиса	Зарплата
IVAN	☞☞☞☞☞☞☞☞	!?!?☞☞☞
PETR	☞☞☞☞☞☞☞☞	☞☞☞☞☞☞☞
OLEG	☞☞☞☞☞☞☞☞	☞☞☞☞☞☞☞

Имя	Карта VISA	Срок
IVAN	1234-5678-9123	04-2010
PETR	2345-6789-4321	09-2012
OLEG	9876-5432-1987	01-2011

Возможная архитектура защиты бизнес-приложений

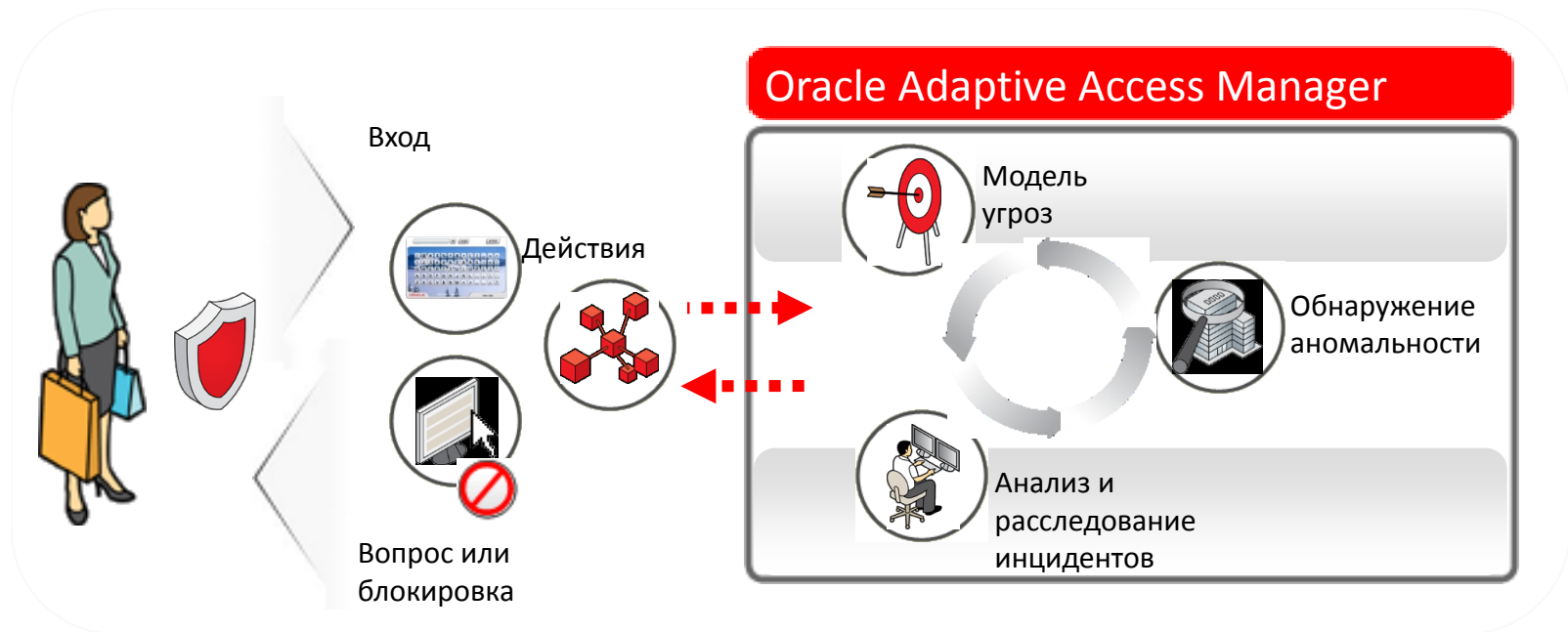


Безопасность на основе оценки риска

Для восстановления доверия и уменьшения риска заказчики интересуются решениями, расширяющими традиционное управление web-доступом (WAM)

- Контекстным анализом действий пользователей для определения степени риска (угрозы)
- Управлением аутентификацией и авторизацией в зависимости от угроз – балансировка между политиками безопасности и степенью риска
- Многофакторной аутентификацией без применения специальных средств
- Технологиями, повышающими доверие пользователей web-каналам
- Быстрым выявлением мошеннических действий, экономя тем самым на расследованиях и судебных издержках

Безопасность на основе оценки риска



- Имя пользователя и пароль верны, **но действительно ли это Мария?**
- Делает ли Мария, **что-нибудь подозрительное?**
- Отвечает ли Мария на дополнительные вопросы, если **риск транзакции** высокий?

ОААМ - анализ рисков

- Профиль пользователя
- Параметры устройства
- IP Geolocation
- Приложения и контекстные данные

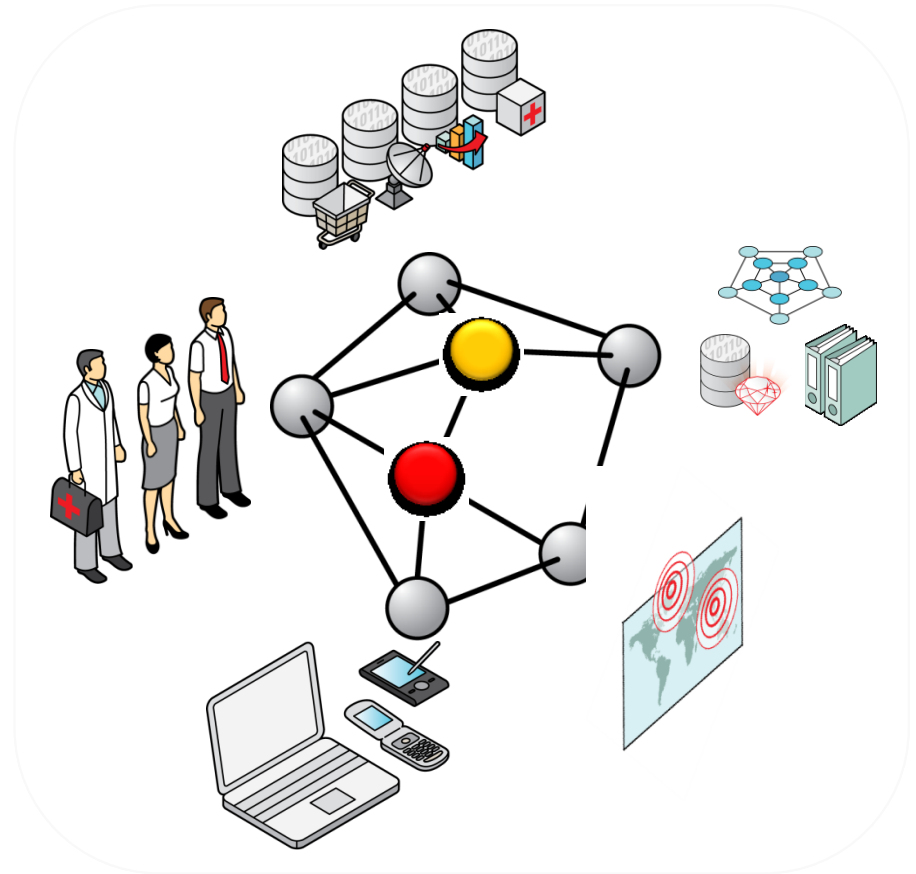


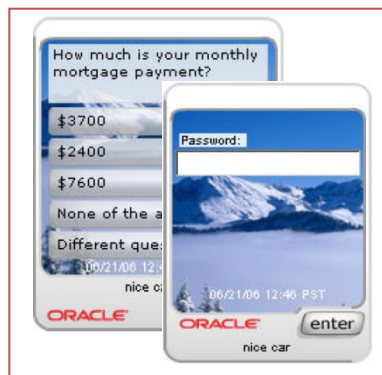
Схема работы ОААМ



RealTime Противодействие краже идентификатора личности и мошенническим действиям



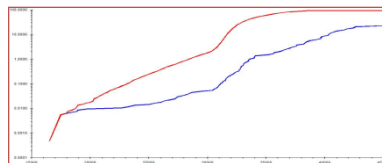
Пользователь



Клиент



Админы



Приложение

Сбор параметров **устройств**

Логика определения уникальности: внутренний алгоритм ОААМ определяет уникальность устройства.

Сбор данных: в страницу встраивается статический код или плагин для сбора характеристик устройств.

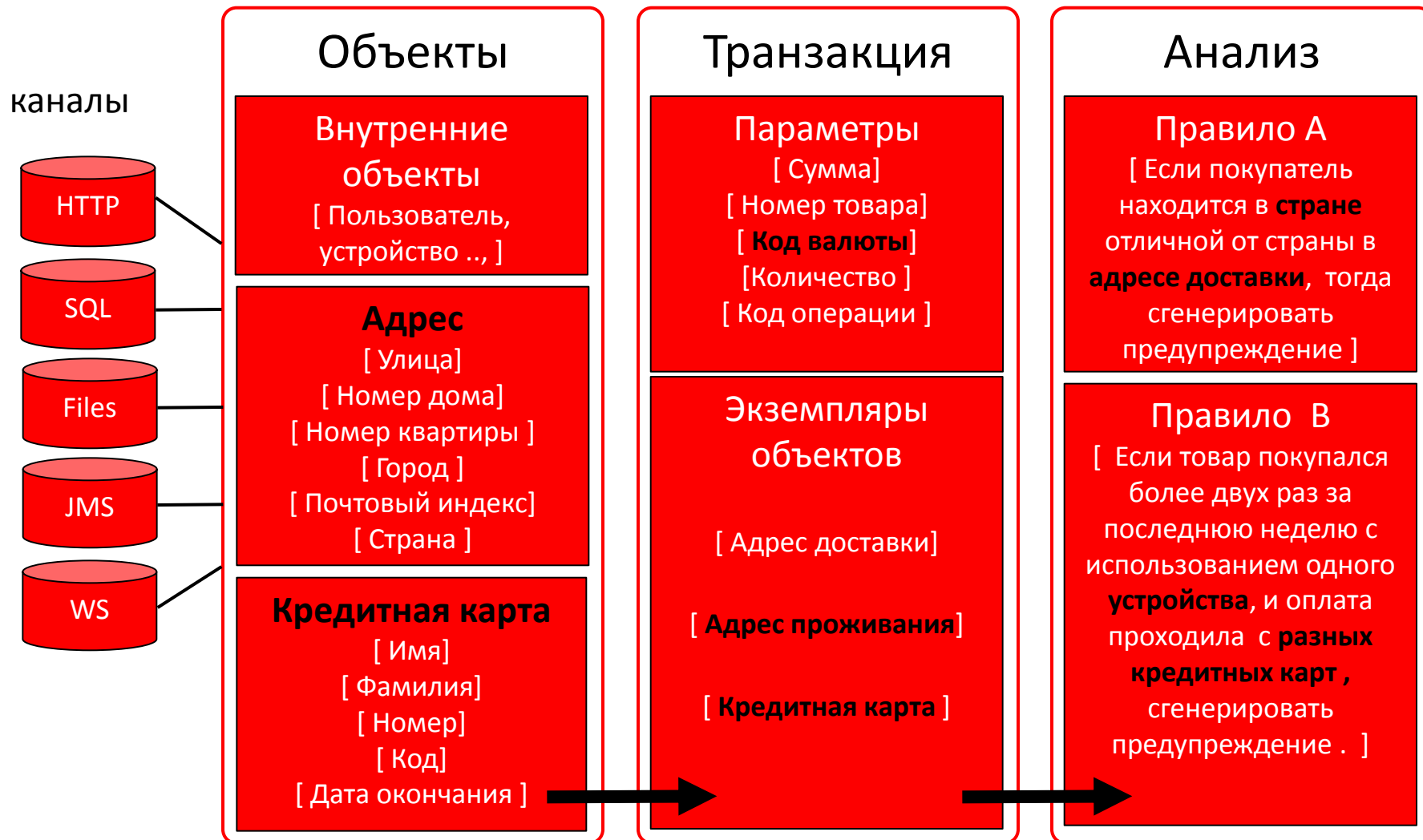
One-Time Secure Cookie (OTSC): для каждой сессии генерируется уникальный токен, проверяется наличие токенов, оставшихся после предыдущих сессий.

Flash Shared Object (FSO): аналогичны OTSC, но могут использоваться повторно в разных сессиях.

HTTP Заголовки: информация о заголовках и агентах в сессии используется для определения уникальности.

Повторная аутентификация: сбор характеристик устройств повторяется в течение сессии неоднократно для предотвращения подмены устройства.

Анализ данных

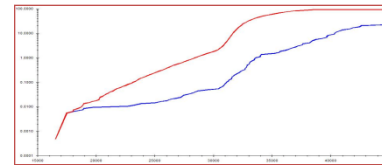


Методы противодействия

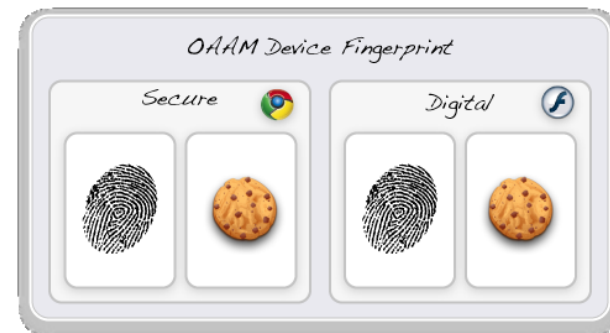
Виртуальные устройства с подтверждением параметров транзакции + OTP



Профилирование поведения пользователя



Анализ характеристик программного обеспечения на рабочем месте пользователя

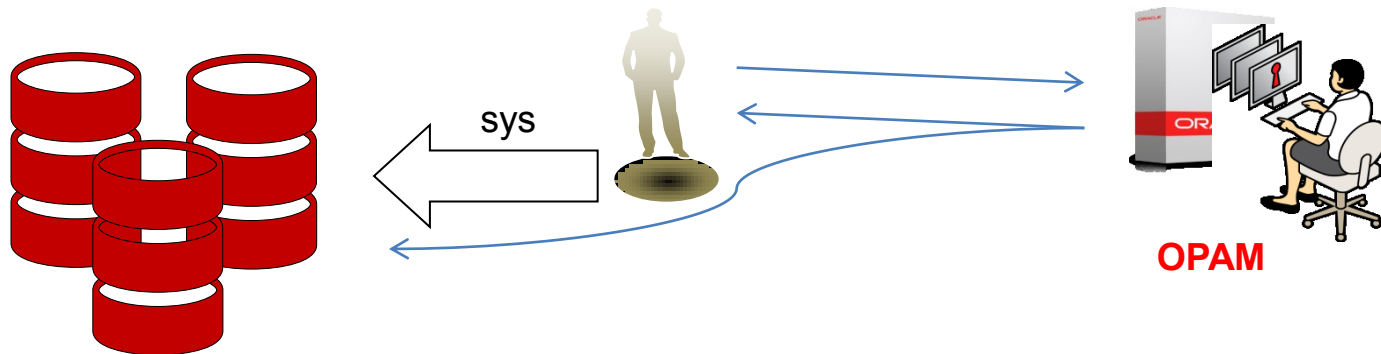


Oracle Privileged Account Manager



Контроль и прозрачность предоставления
административного доступа

Oracle Privileged Accounts Manager



Базы данных

- Возможность применения единых политик безопасности как к обычным, так и к привилегированным (разделяемым) учетным записям
- Устранение (уменьшение) потенциальных угроз от инсайдеров
- Упрощение соответствия требованиям регуляторов
 - Сертификация «владения» привилегированными учетными записями

Oracle Access Management Mobile & Social

Расширение архитектуры предоставления доступа с учетом современных тенденций: **мобильность**, **облака** и **социальные** сервисы



Безопасность
для мобильных
устройств



Интеграция с
социальными
сетями

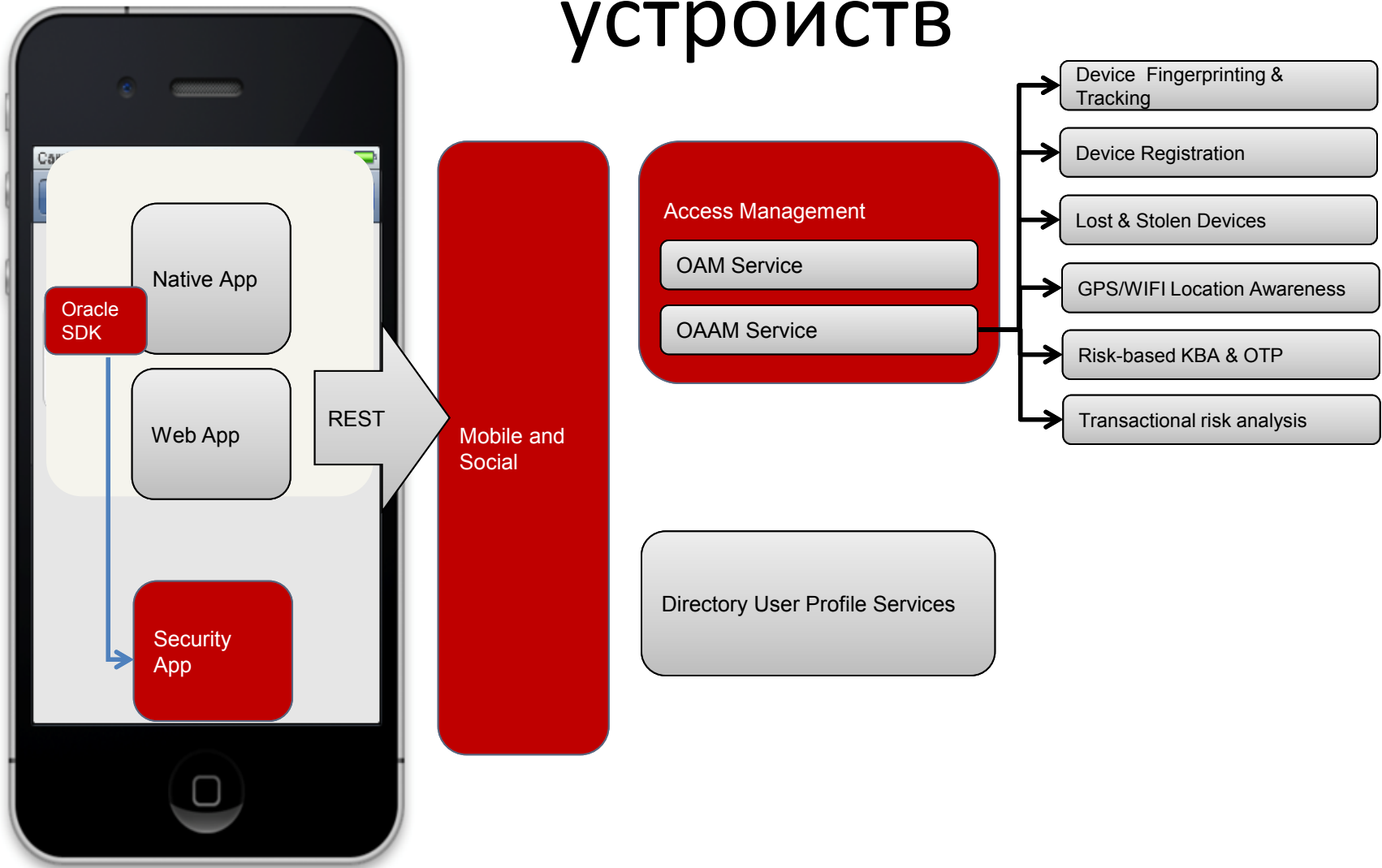


Безопасность
для облачных
вычислений



Поддержка
стандартов

Безопасность для мобильных устройств



Single Sign-on для мобильных устройств



Вопросы...

