



Защита мобильных устройств Oracle Mobile Security Suite

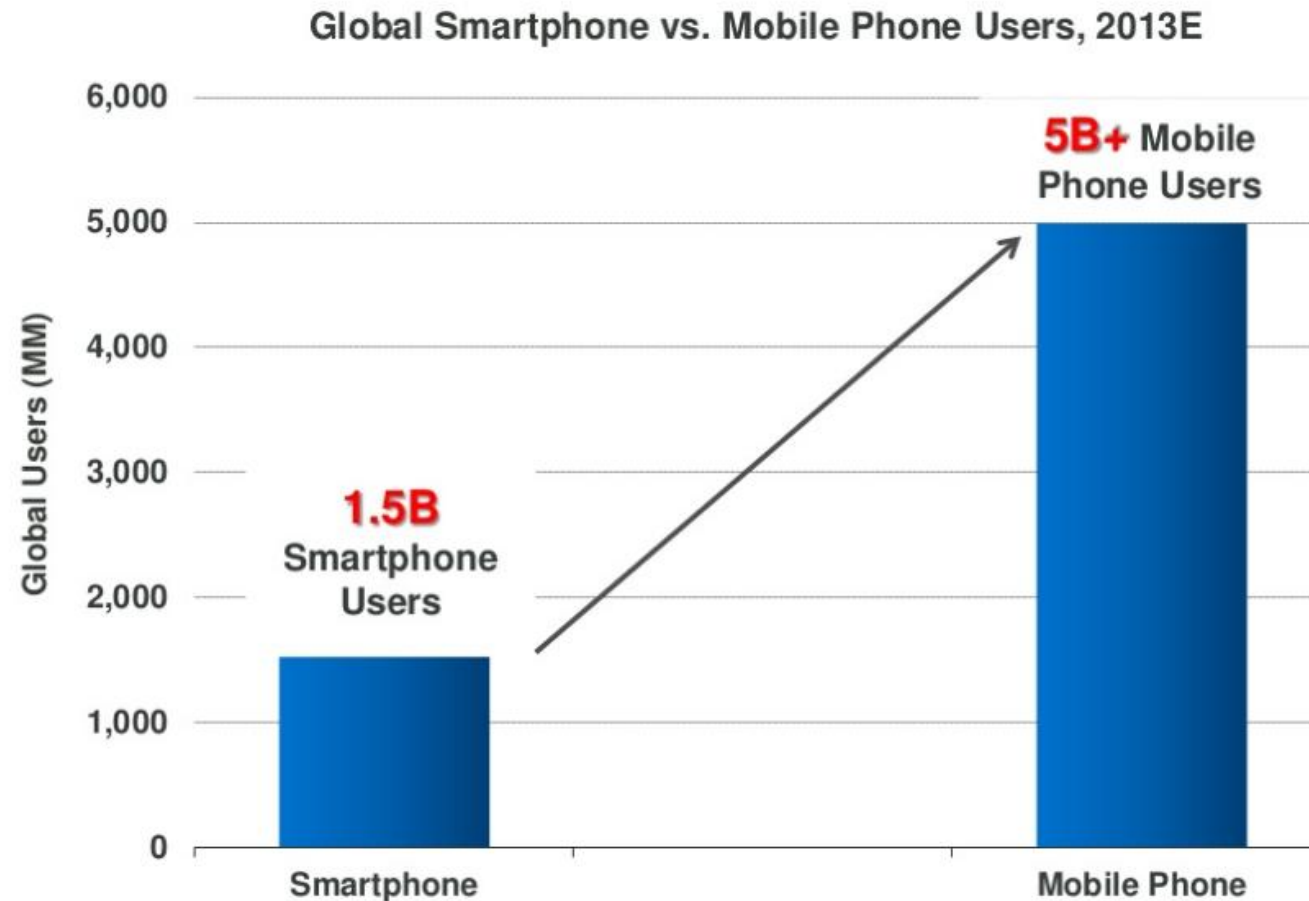
Natalia Kusova,
Senior Sales Consultant, Oracle

Oracle Security Solutions



Смартфоны + Планшеты—Новые устройства

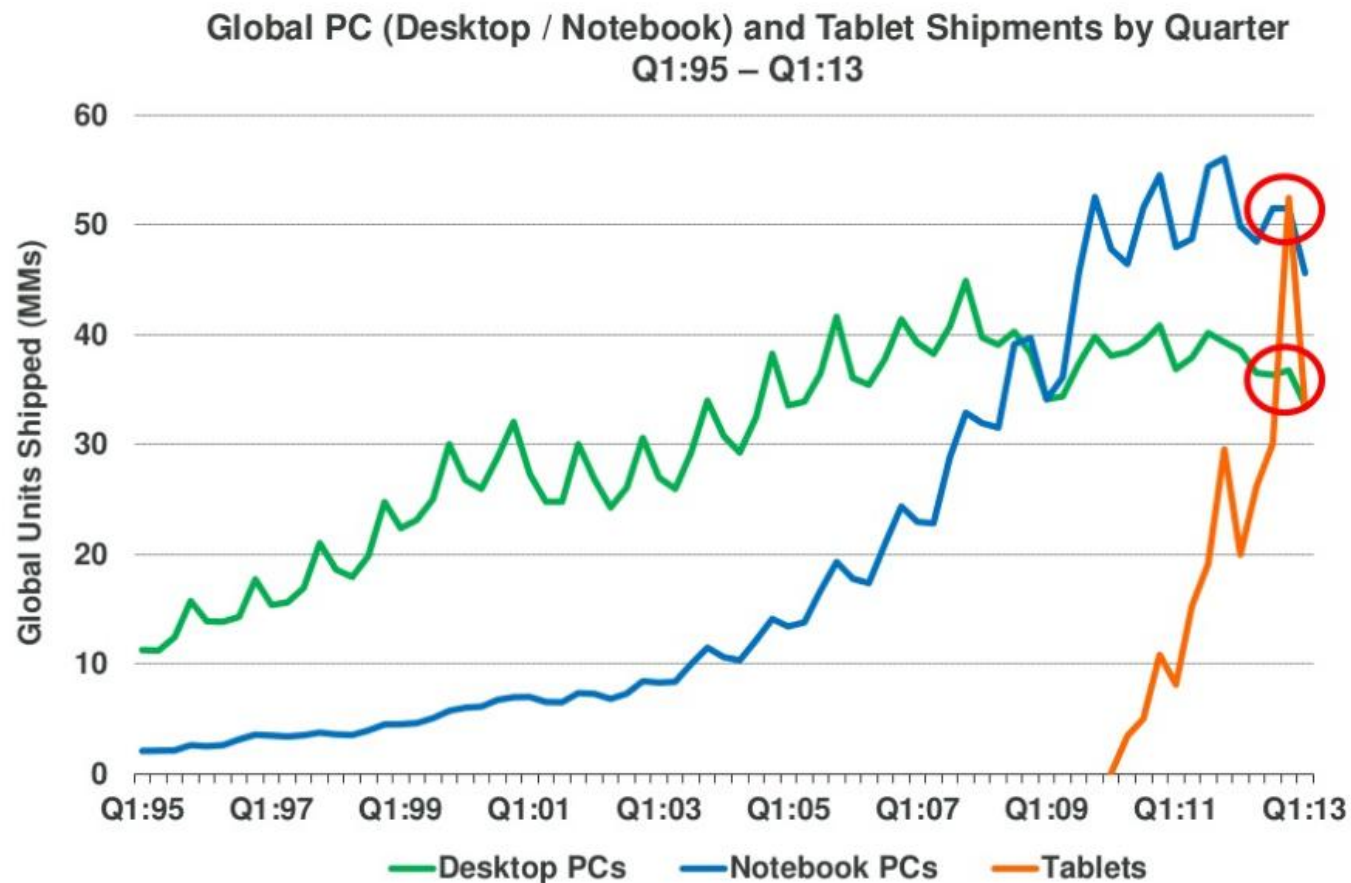
3-4х кратный потенциал роста количества смартфонов



Source: KPCB

Смартфоны + Планшеты—Новые устройства

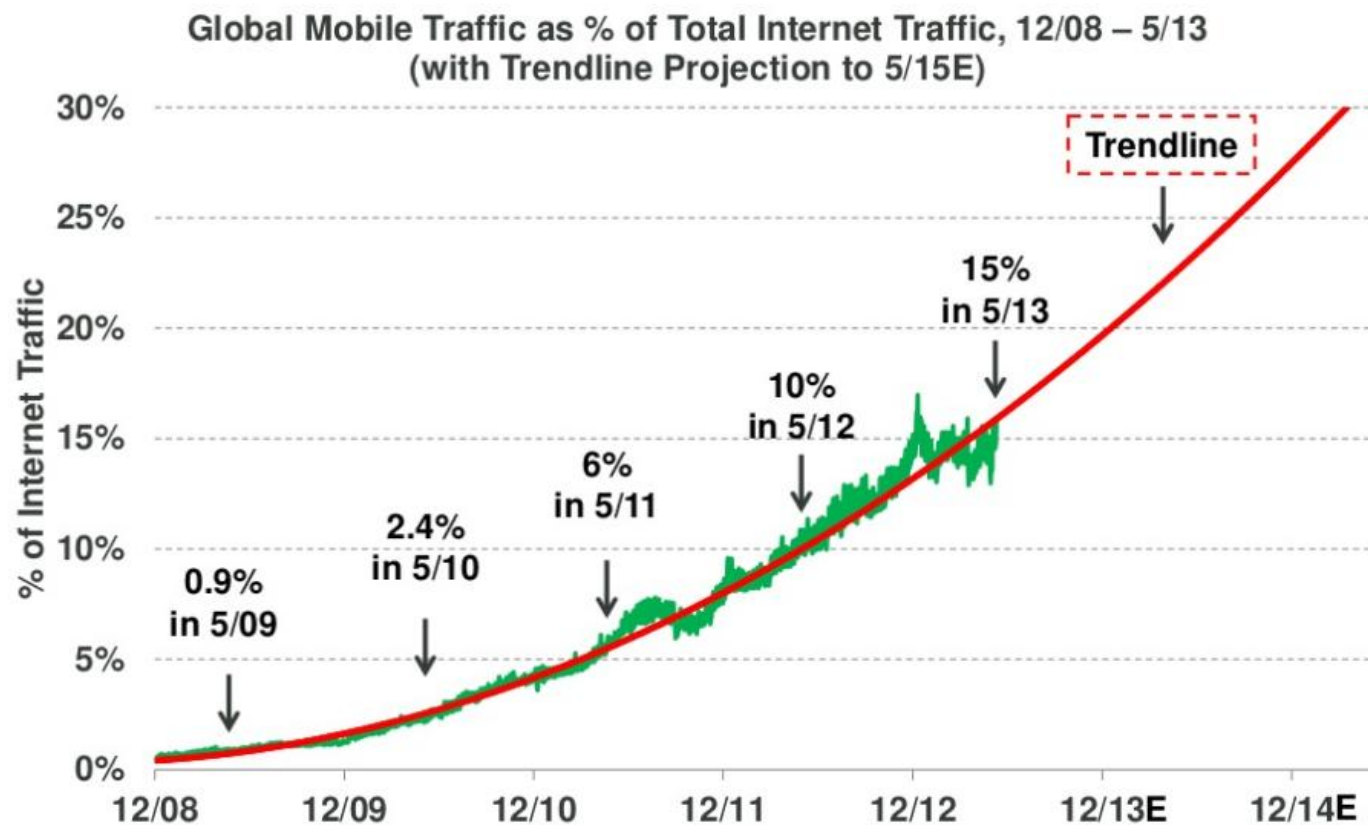
Поставки планшетов превзошли настольные ПК и ноутбуки



Source: KPCB

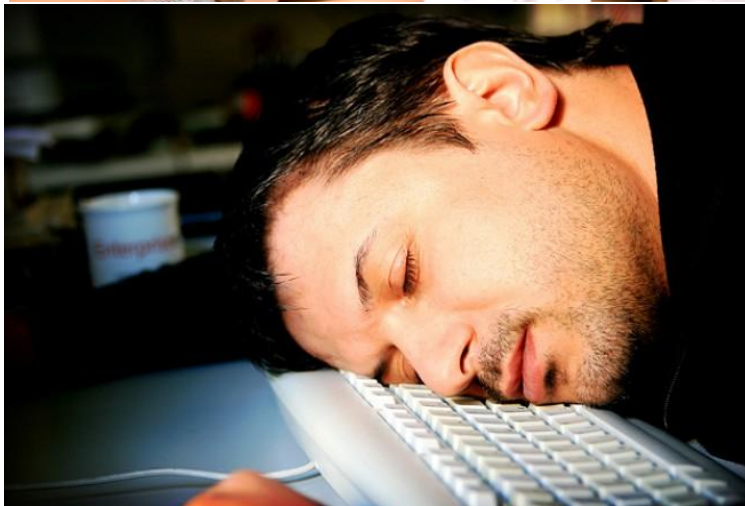
Мобильный трафик как % от общего интернет трафика

Рост 150% за год. Огромный потенциал роста.



Source: KPCB

Бизнесу тоже это интересно – надо повышать производительность труда сотрудников



**Для офиса предел почти достигнут;
надо идти дальше!**



Что говорят наши клиенты

Защищенный доступ с мобильных к приложениям предприятия



- Повышается использование мобильных устройств на предприятиях, BYOD становится стандартом и BYOD требует пользователь ориентированного решения (не устройство ориентированного)
- Защита доступа к приложениям предприятия представляет новые риски безопасности, т.к. телефоны теряются, их могут украсть и т.д.
- Клиенты ищут решение, которое разделить персональные и корпоративные данные и приложения
- Ключевое требование организаций – защитить основные продуктивные приложения и работать с заказными приложениями
- Существующие на рынке мобильные решения требуют дублирования средств защиты мобильного доступа

Что такое BYOD?

Bring Your Own Device (не путать с *Bring Your Own Drink*)

- BYOD – тренд Принеси свое собственное устройство. Компания разрешает сотрудникам использовать собственные устройства для рабочих целей. Возникает необходимость разделить данные на корпоративные и личные.
- При появлении BYOD для мобильных устройств появились задачи отделения корпоративных данных, отзыва настроек, ПО и данных, без полной очистки устройства.

ОПРЕДЕЛЯЯ Мобильную безопасность



Среда разработки мобильных приложений

- Широкая стратегия разработки и защиты мобильных приложений
- Включает доставку корпоративных приложений на мобильные устройства
- Требуется наличие платформы управления учетными данными

**Mobile Enterprise
Application
Platform
MEAP**

Защита доступа к приложениям

- VPN/SSL доступ к корпоративной сети
- Требуется интеграции мобильных приложений и защиты API
- Сообщения и уведомления
- Требуется наличия платформы управления учетными данными

**Secure Mobile
Back-end As A
Service
MBaaS**

Управление устройством

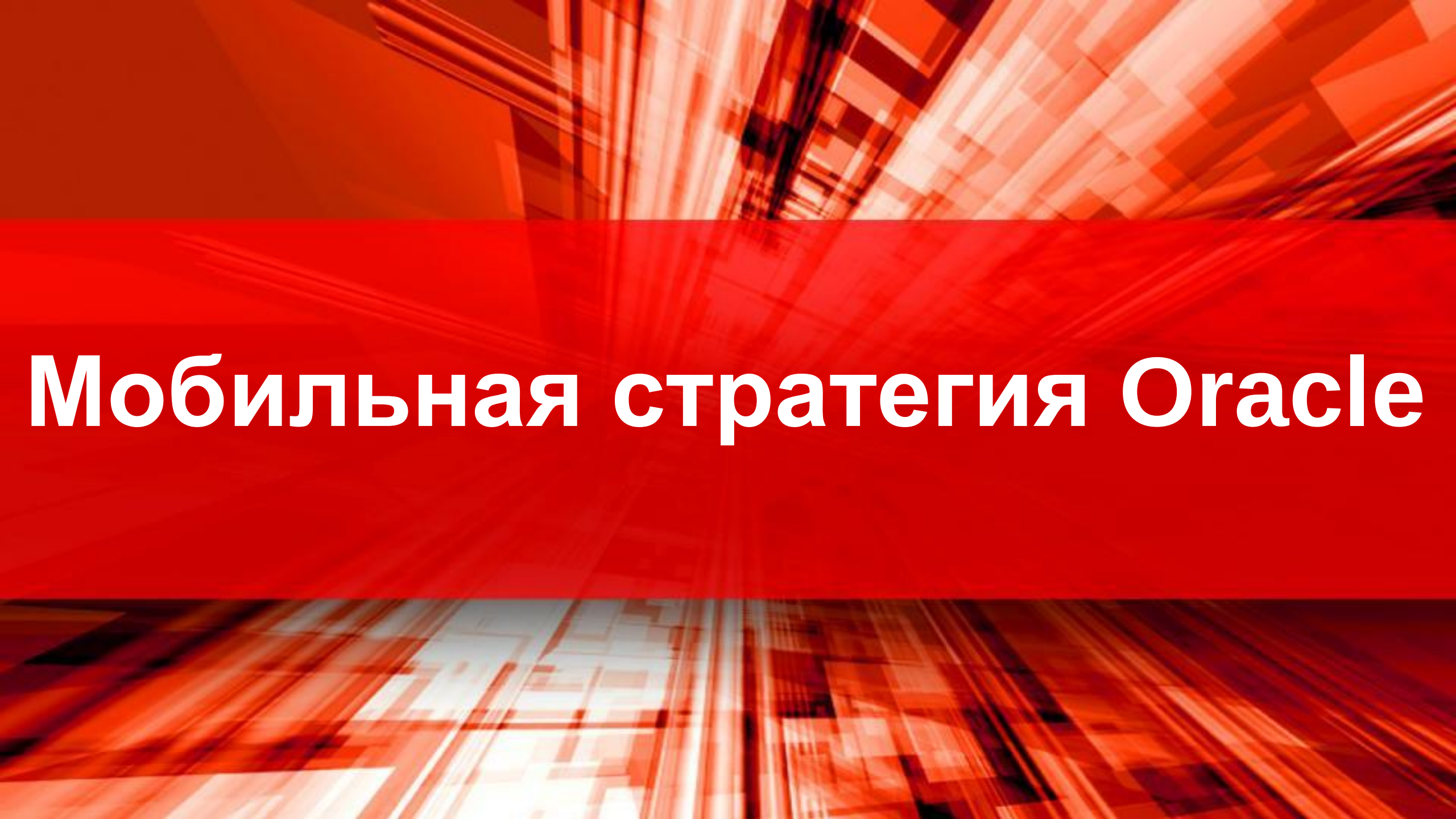
- В центре устройство
- Цели сладить с устройством
- Монолитное управление данными
- Обычно требует особый набор удостоверяющих политик

**Mobile Device
Management
MDM**

Управление приложениями

- Разделение личных и корпоративных приложений и данных
- Создание и управление безопасным контейнером приложений и данных
- BYOD ориентированно
- Использует существующие сервисы идентификации

**Mobile
Application
Management
MAM**



Мобильная стратегия Oracle

Построение своих
собственных
приложений

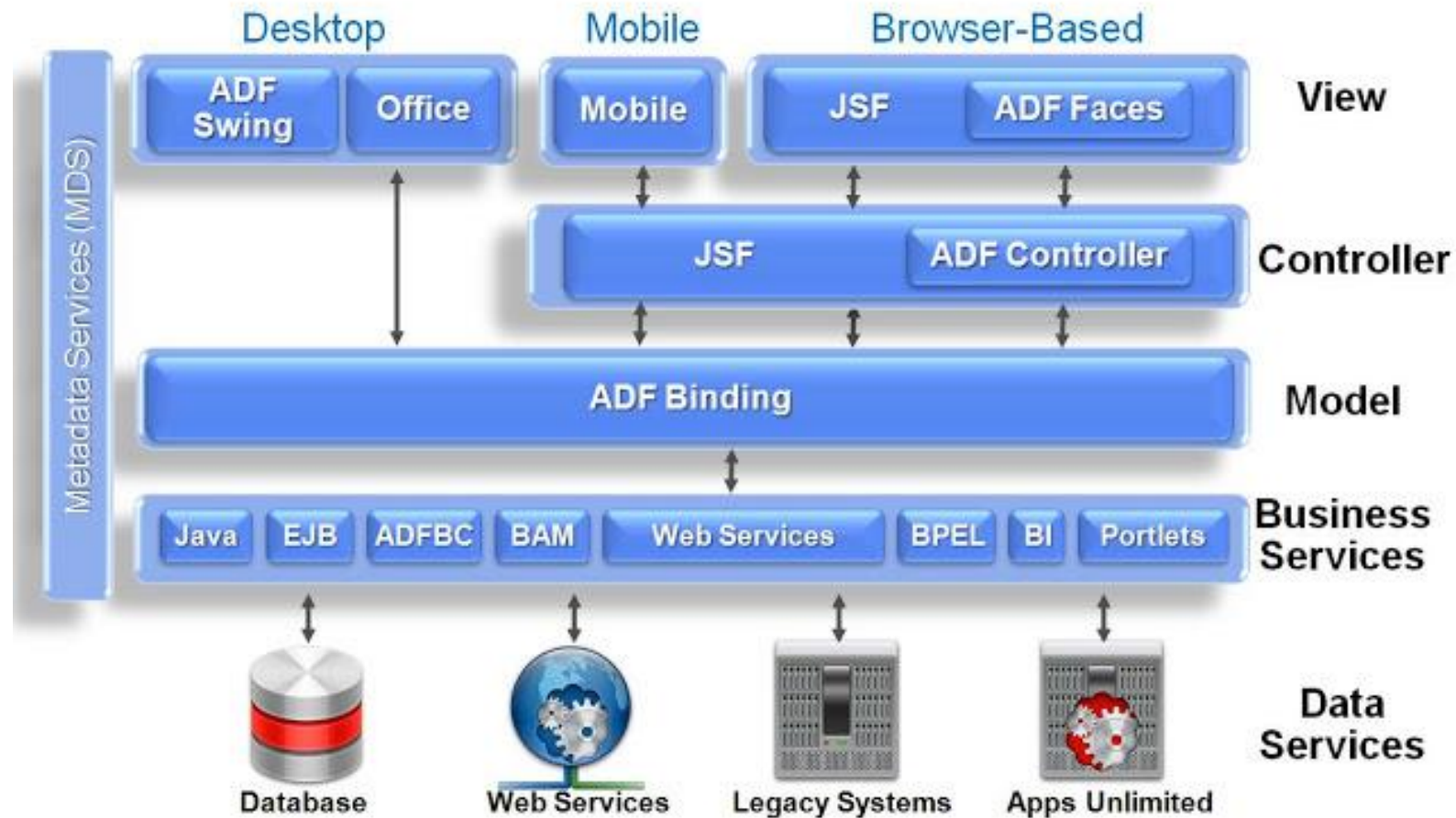
Мобильные
приложения Oracle



Мобильная стратегия **ORACLE**

Мобильная стратегия Oracle

Готовые приложения Oracle и ADF Mobile



The background features a complex, abstract design with a central horizontal band of solid red. Above and below this band are areas filled with a dense, overlapping pattern of red and orange squares and rectangles, creating a sense of depth and movement. The overall color palette is dominated by warm tones of red and orange.

Oracle Mobile Security Suite

Развитие платформы мобильной безопасности

Oracle покупает Bitzer Mobile!

- Саннивейл, Калифорния, компания, основана в 2010
- Направлена на упрощение и защиту мобильности предприятия, предлагая MAM решение
- Несколько известных клиентов

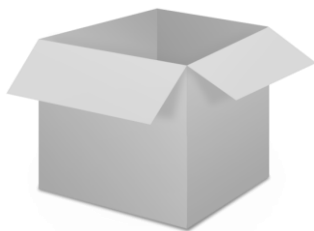


Стратегия

МОБИЛЬНОЙ БЕЗОПАСНОСТИ

Oracle

КОНТЕЙНЕР



Изолирует корпоративные данные, поддерживает удаленную очистку, предотвращает передачу данных

КОНТРОЛЬ



Защищает приложения и соединение, корпоративное хранилище приложений

УДОБСТВО



Доступ на основе ролей, запросы самообслуживания, SSO, обнаружение мошенничества

MOBILE SECURITY SUITE

ORACLE

Взгляд Oracle на безопасность мобильных устройств

Требования к безопасности мобильных устройств



Аутентификация

Шифрование при
хранении

Шифрование при
передаче

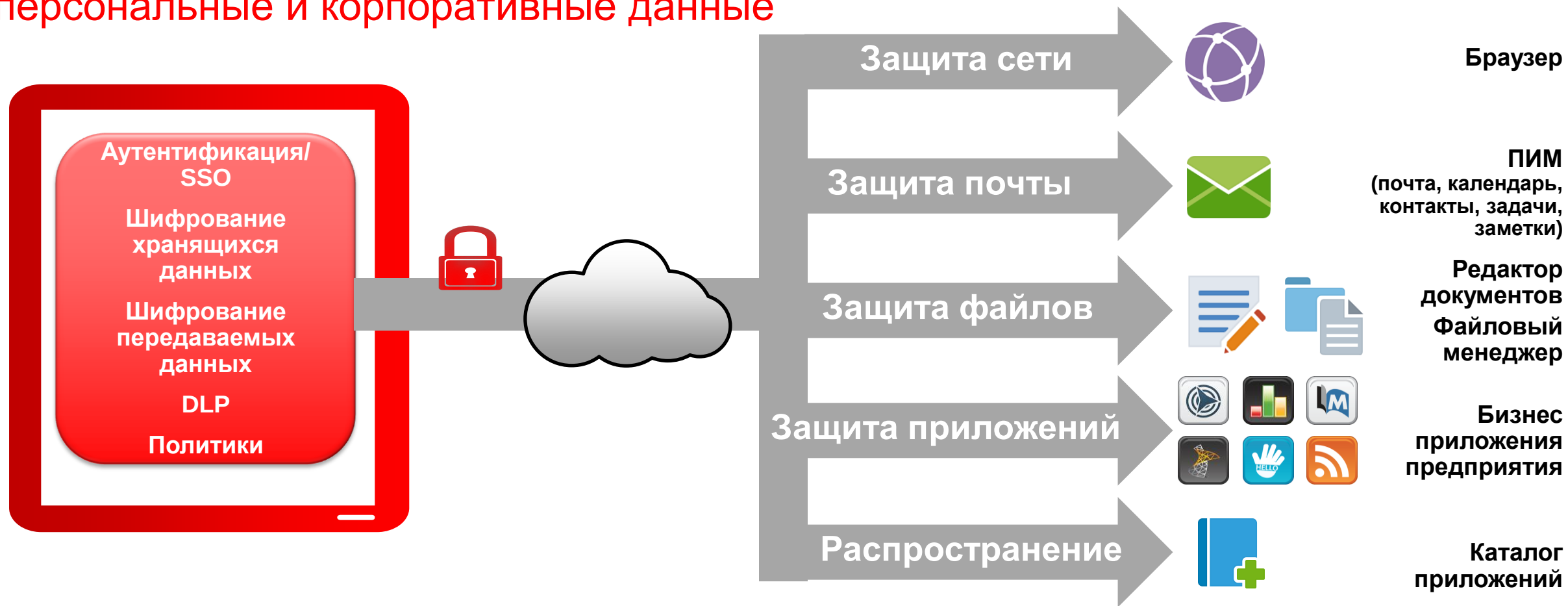
Контроль утечки
данных

Применение политик

- Разделение личных и корпоративных данных
- Решение ориентированное на приложения – предотвращает блокировку устройства
- Расширение платформы Identity Management для управления приложениями и контейнерами
- Расширение платформы Access Management для мобильных устройств и приложений
- Мобильные приложения Oracle/ADF защита по умолчанию используя сервисы безопасности

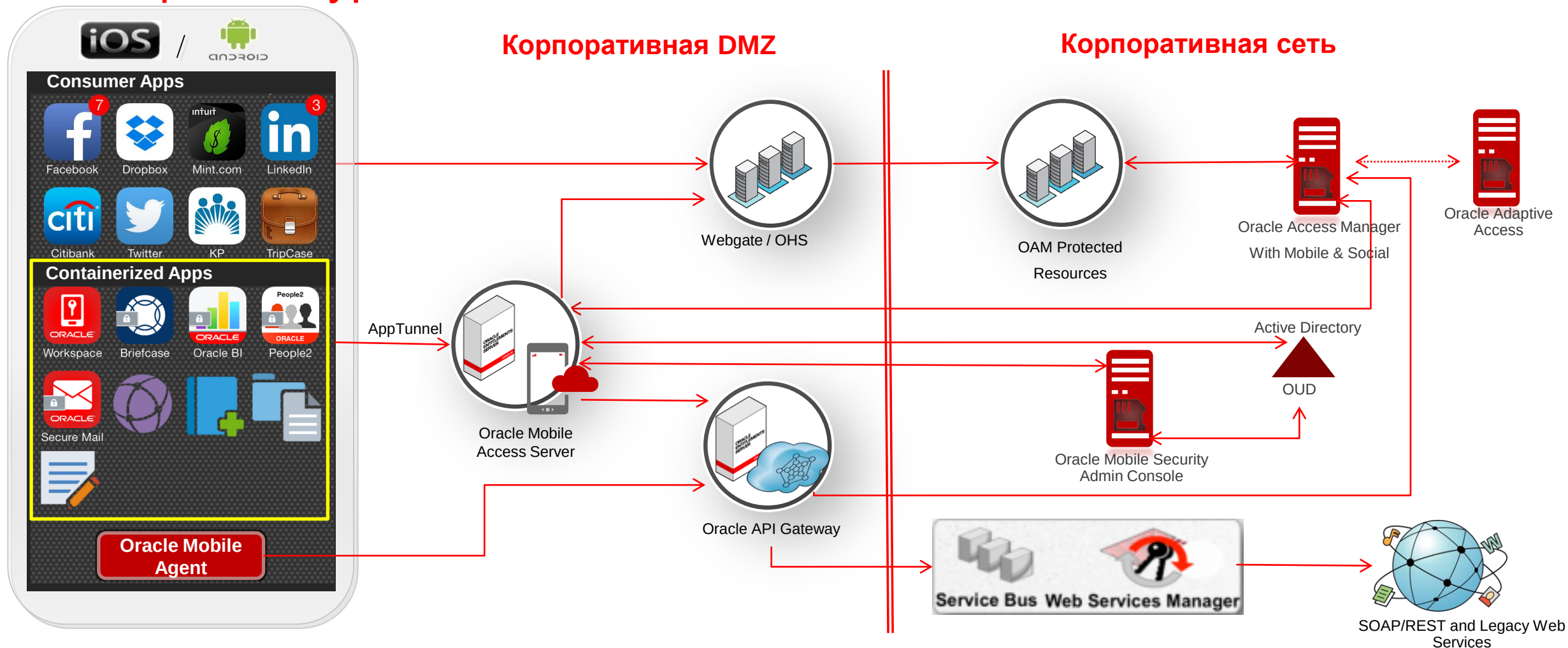
Мобильное решение Oracle

Защищает рабочую область мобильных устройств – Разделяет персональные и корпоративные данные



Oracle Mobile Security Suite

Архитектура



Защита соединения



- Защищенное соединение с серверами приложений предприятия
- Без VPN и дополнительной защиты сети (такой как IPSEC), энергоэффективно
- Поддержка сторонней и идентификации через социальные сети
- Обеспечивает контекстный и на риск-зависимый доступ к приложениям предприятия
- Регистрация устройства и установка

AppTunnel – туннель приложения

Нет необходимости в VPN уровня мобильного устройства

- Взаимно аутентифицированный SSL туннель
 - Преимущества перед IPSec = сохраняет свое состояние между сетями
- Защита от мошеннических приложений
- Доступ к внутренней сети только для приложений из «белого» списка
- Оптимизированно для мобильного трафика
 - Сжатие для повышения пропускной способности и производительности
- Прозрачное переключение между WIFI и 3G

Шифрование

При хранении и передаче

- Шифрование сертифицированное FIPS140-2 Level 1
 - OpenSSL FIPS Object Module Версия v2.0 сертификат #1747
- Данные, хранящиеся на мобильном устройстве
 - File store, database (sqlcypher), cache, user prefs...
- Передаваемые данные (AppTunnel)
- Шифрование используемое в MDM решениях зависит от производителя устройства (Apple, Samsung KNOX/SAFE...)

Защита от утечки данных

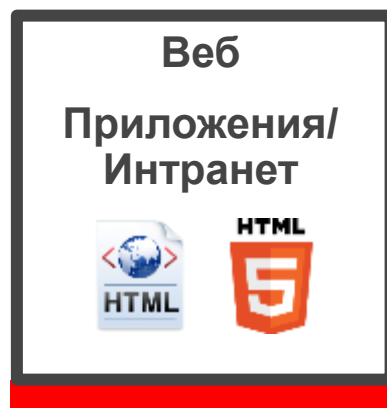
Полный набор средств управления для кросс-платформенных приложений на основе политик

Backup	Copy/paste	Email	IM	Video chat	Social share	Print	Open In	AirDrop	Save to media gallery	Save to contacts
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

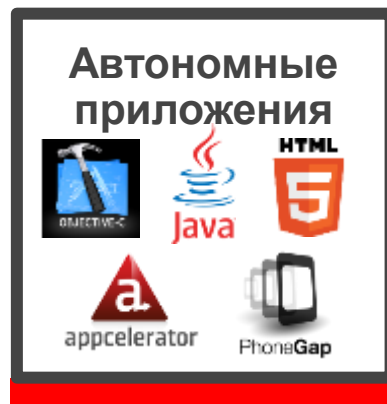
Контейнеризация приложений

Oracle Mobile Security Suite

Защищает приложения и данные



Безопасный
браузер



Контейнеризация



Инструмент для контейнеризации приложений

Идеально подходит для своей разработки или для сторонних приложений, для создания “доверенного рабочего пространства”

- ▶ Общая встроенная аутентификация Windows (IWA)
 - ▶ SSO or layered
- ▶ Общий туннель приложений– преимущества перед мобильным VPN
- ▶ Общие ключи шифрования– никогда не хранятся на устройстве
- ▶ Общая среда для политик– разные политики для разных пользователей
- ▶ Ограничение передачи (открыть в, почта, копирование/вставка...) только для приложений “доверенного рабочего пространства”

Не подписанные автономные приложения



Инструмент для контейнеризации



Контейнеризированные приложения



Распространение пользователям

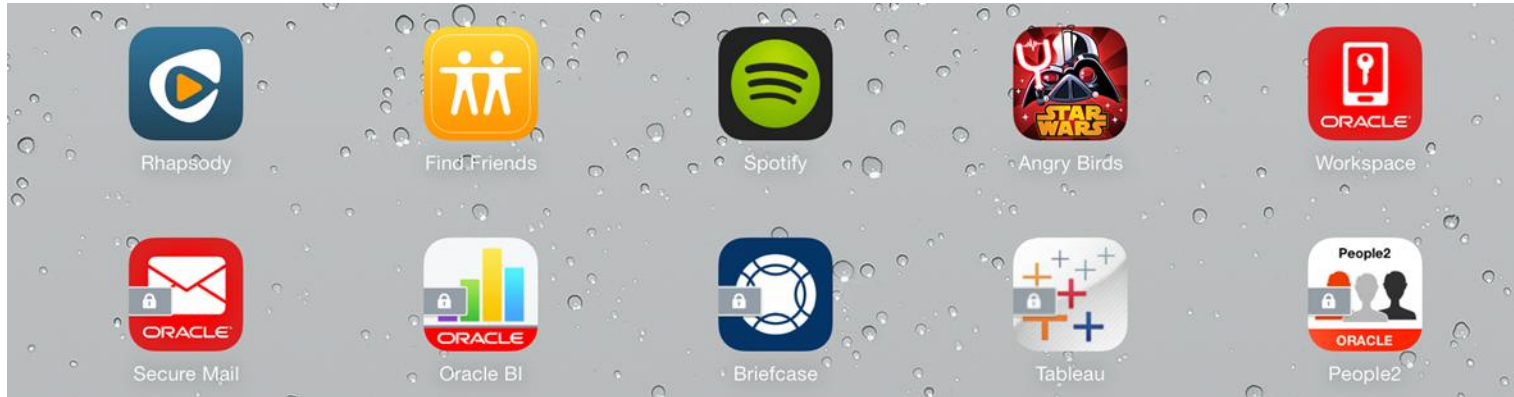
Распространение на предприятия

Доступно для:



Защита автономных приложений

Модель делегированной безопасности с контейнеризированием приложений



- Контейнеризация приложений добавляет слой безопасности для заказных и своих приложений после разработки
- Отделите обеспечение безопасности от разработки приложений
- Подход на основе инъекции. Без необходимости иметь исходный код.

Жизненный цикл контейнера



Обзор защищенного контейнера

- Используются различные механизмы для определения **Jailbreak** и **root** устройств.
- Код основных механизмов защиты обфусцирован / выполнен на C что бы затруднить обратный инжиниринг.
- Ключи управляются в памяти и безопасно вычищаются:
 - Учетные данные пользователя очищаются после получения ассоциированного КЕК.
 - КЕК очищается после расшифровки Data Protection Root Key.
 - Data Protection Root Key очищается после расшифровки Data Protection Keys.
 - Data Protection Keys индивидуально очищаются когда больше не нужны.

Заключение

- Для повышения продуктивности Необходимо дать сотрудникам новые мобильные приложения, а не просто защищенный доступ к почте (подход Blackberry)
- Руководители IT хотели бы использовать универсальные или предынтегрированные решения
- Мобильная безопасность на базе MDM & VPNs не решает всех задач защиты и раздражает пользователей
- Мобильный контейнер это часть новой архитектуры обеспечения безопасности мобильных

ORACLE®