ORACLE

MARVEL дистрибуция

Обеспечение защиты мобильных устройств. Программа сертификации средств безопасности Oracle

Андрей Гусаков, руководитель группы консультантов по Enterprise Security

Москва, 25 марта 2014 года

МЫ НАБЛЮДАЕМ НАИБОЛЕЕ ЗНАЧИТЕЛЬНОЕ ИЗМЕНЕНИЕ IT-АРХИТЕКТУРЫ ЗА 20 ЛЕТ

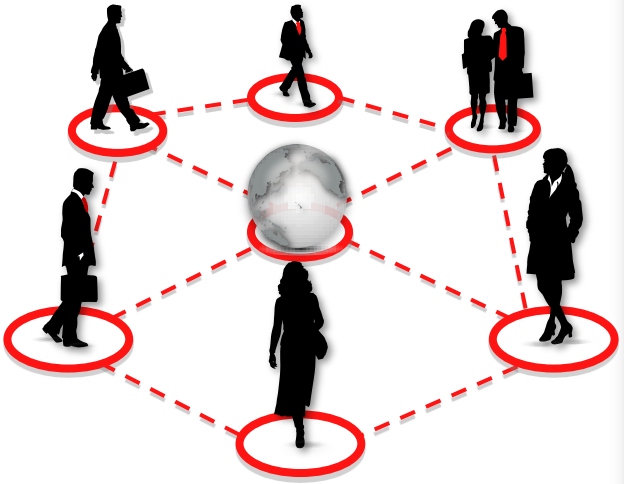
Тренд – Использование мобильных устройств

- Персонифицированный контроль
- Многоканальный маркетинг
- Mobile Device (MDM) и Mobile Applications (MAM) Management
- Единая среда управления

Тренд – Использование облачных сервисов

- Облачные хранилища IDs для SaaS
- Облачные порталы доступа
- Аутентификация как сервис
- Самообслуживание пользователей
- Полноценные аудит и отчетность

Тренд – Использование социальных IDs



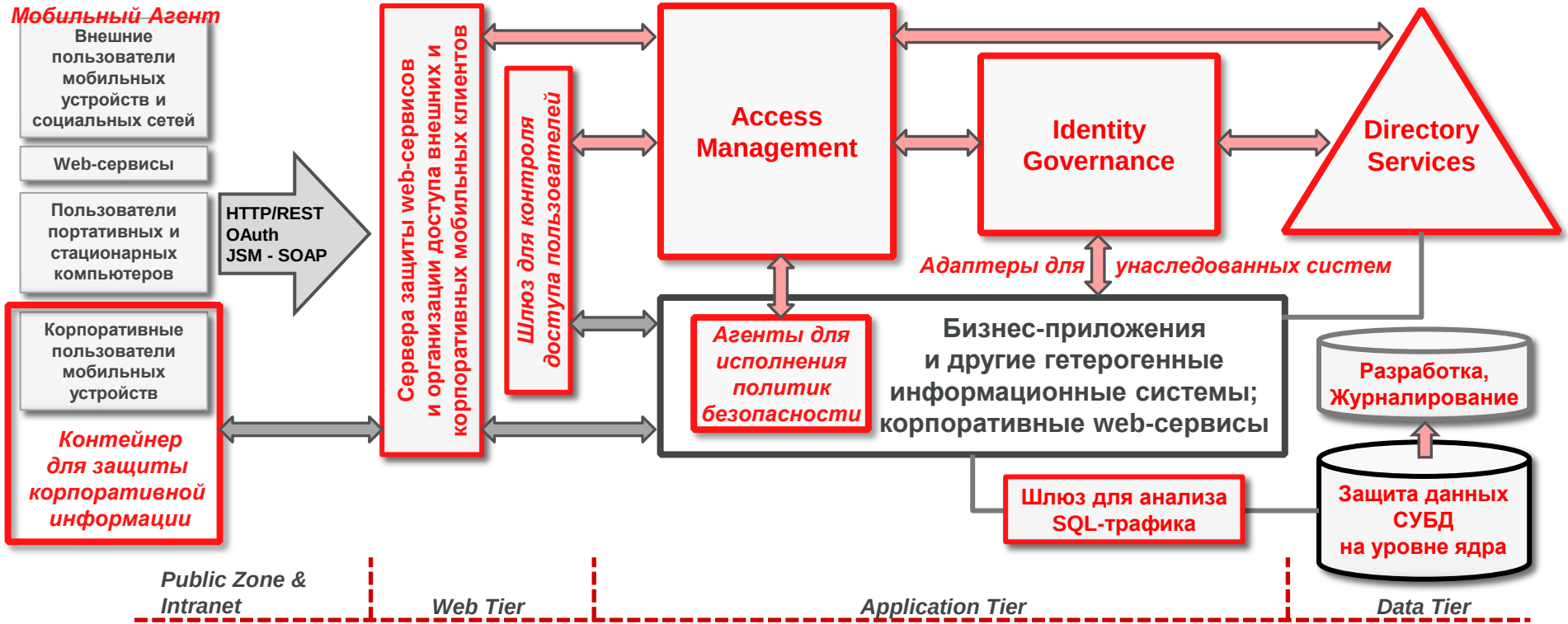
- Проще регистрация и взаимодействие
- Растет роль IdPs
- Протоколы OAuth & OpenID
- Растет опыт
- Доверие надо заслужить

Проблемы защиты приложений

Типичная «исходная позиция»

Знакомство со средствами защиты приложений

Технологические методы управления рисками безопасности



Инструменты защиты на службе бизнеса

Пример: Oracle Access Management Mobile & Social

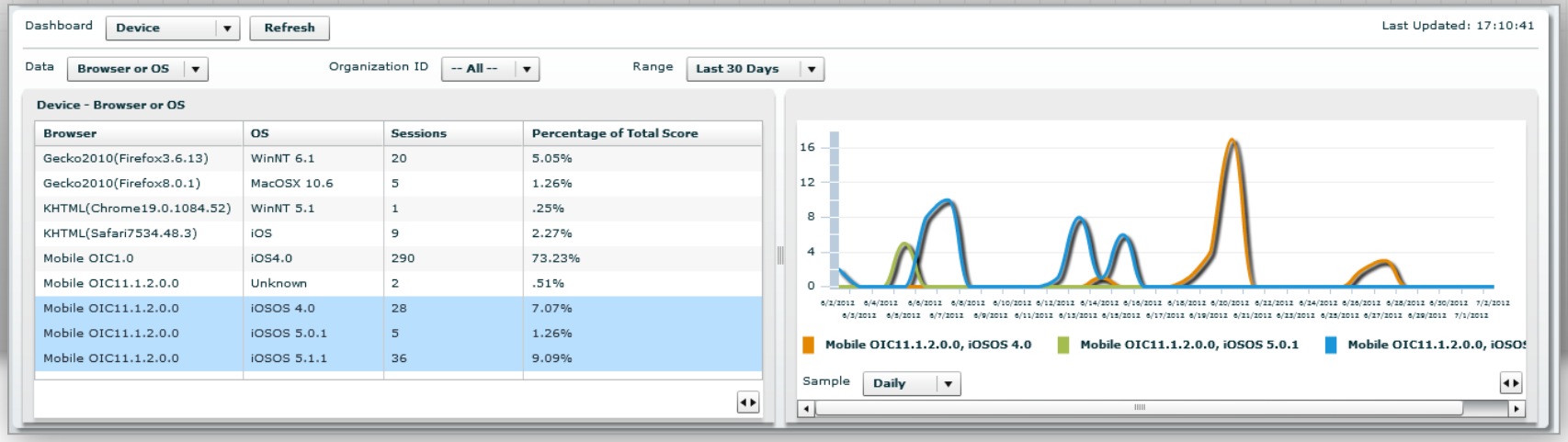
- Платформа для безопасности мобильных устройств
  - Аутентификация и SSO
  - Сбор данных с устройств и контроль доступа с учетом риска
  - Mobile SDK
- Интеграция с социальными ID
- REST/Cloud интерфейсы

Наглядная мобильность

Текущие и исторические данные по попыткам доступа и оценкам риска

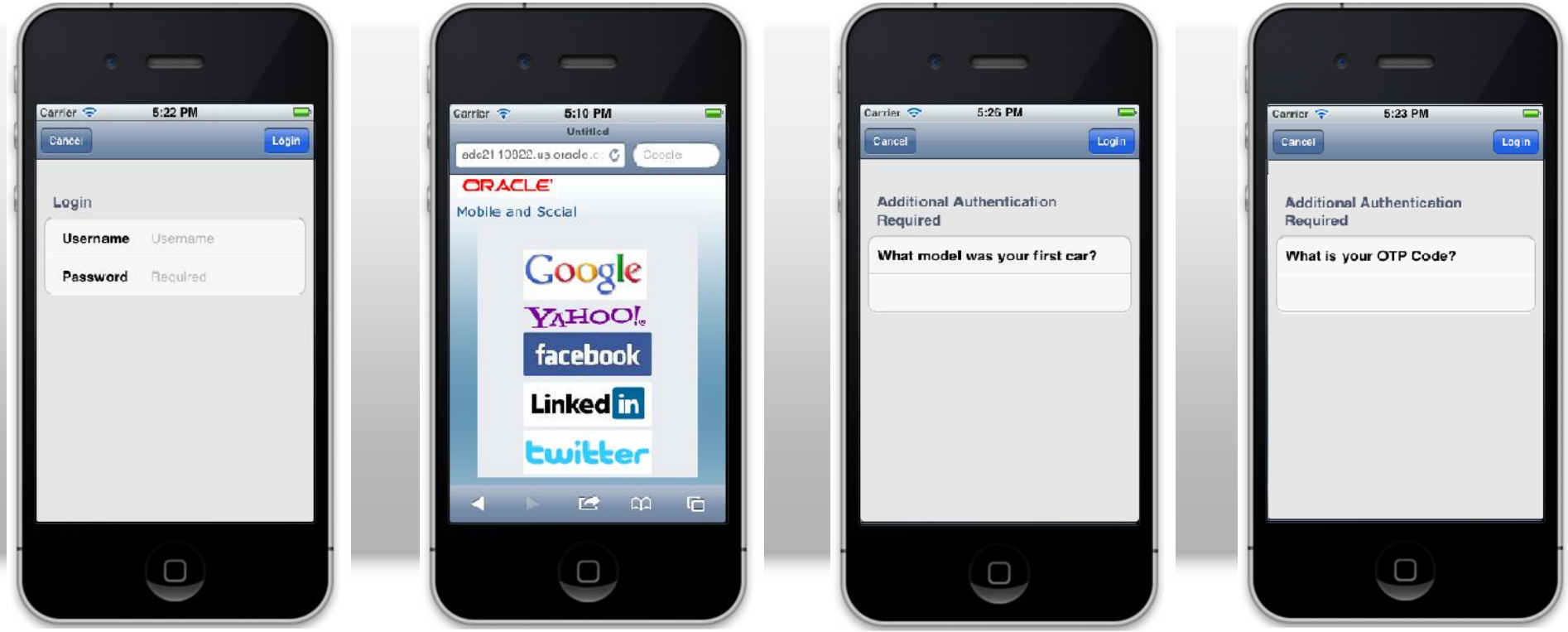
Row	Session ID	Alerts	User Name	Device ID	Device Type	Client Application Name	Longitude	IP Address	Location	Authentication Status	Session Date	Post authentication Score	Post authentication Action
6	104		ted	103	Mobile device	OICSecurityApp	40.68906	103.37.240.35	United States, Cali...	Success	6/27/2012 4...	0	Allow
7	103		tates	103	Mobile device	OICSecurityApp	40.68906	124.240.10.37	United States, Cali...	Success	6/27/2012 4...	300	Challenge
8	102	Medium Alerts: (1)	rivat1	102	Mobile device	OICSecurityApp	46.68906	10.240.37.124	Private, Private, P...	Blocked	6/27/2012 2...	1000	Block
9	101		csrm1	101	Mobile device	OICSecurityApp	40.89906	130.35.103.33	United States, Cali...	Pending	6/27/2012 2...	300	Challenge

Анализ характеристик устройств, включая версии OS и SDK



Мобильная аутентификация

Множество вариантов для устройств, приложений, клиентов

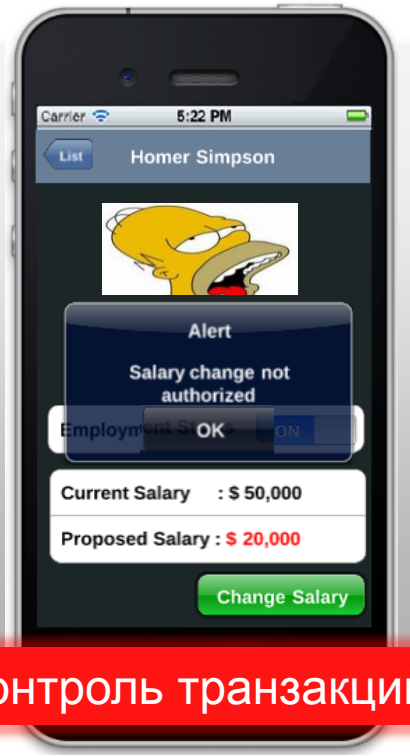


SSO на устройстве

Единая среда для всех мобильных приложений (web & native)

Авторизация с учетом контекста

- Политики оценки содержимого запросов
- На основе стандартов
- Полный аудит
- Реализация без внесения изменений в код приложений

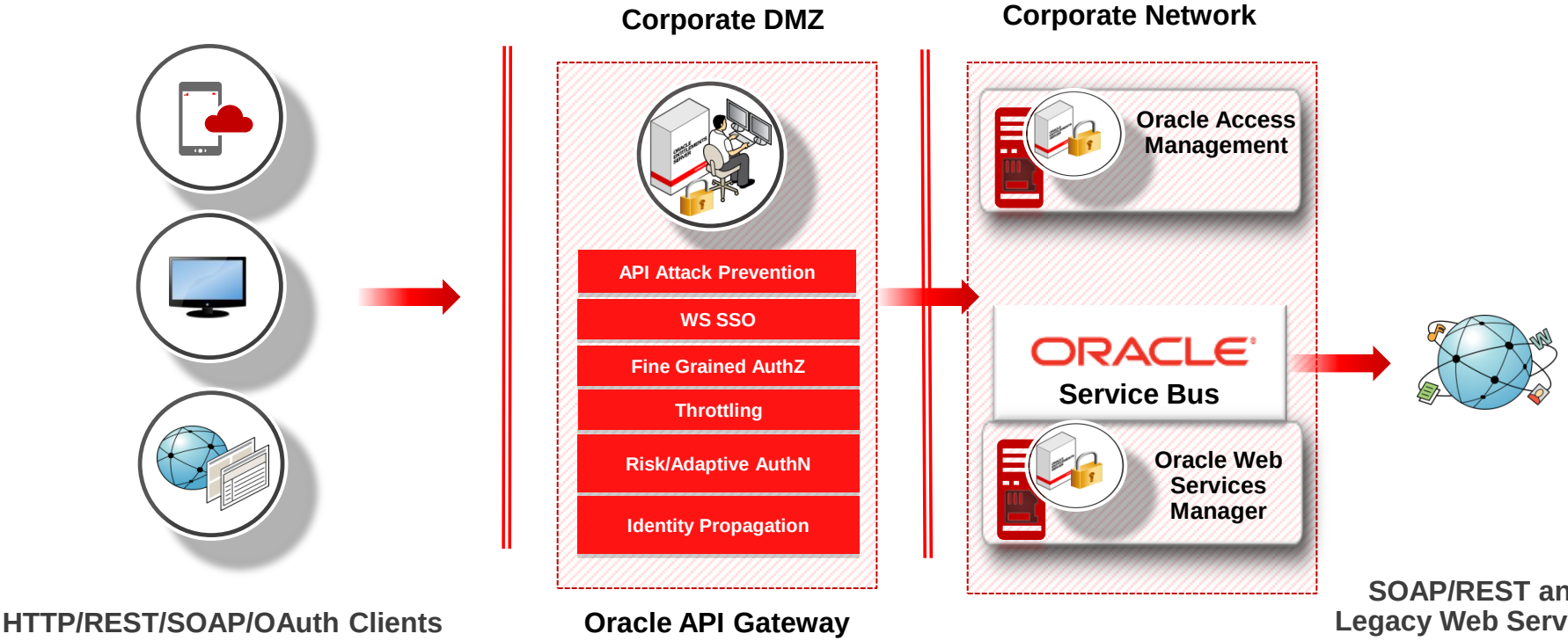


Маскирование данных

Контроль транзакций

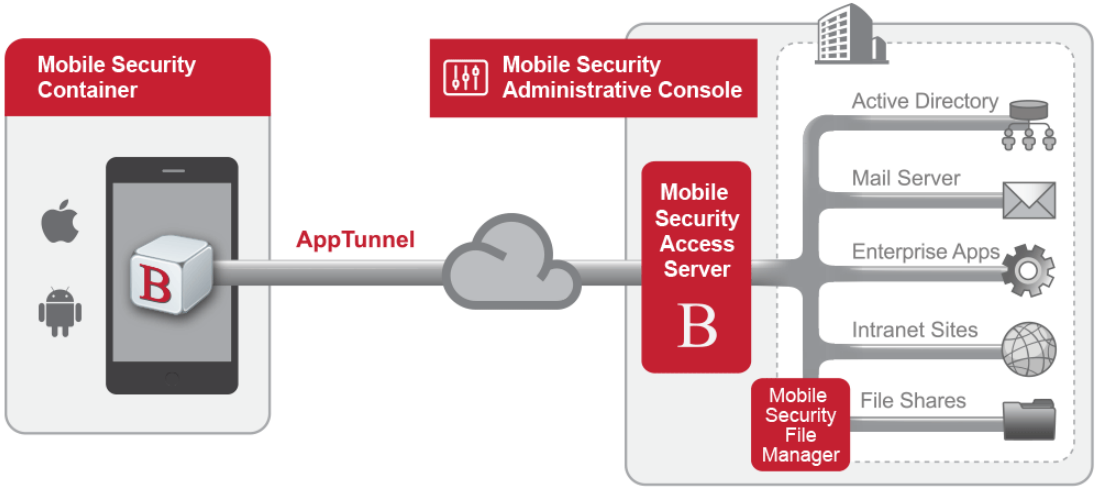
Oracle API Gateway

Первая линия обороны интеграционных интерфейсов



Oracle Mobile Security Suite

Защита мобильных корпоративных приложений и данных

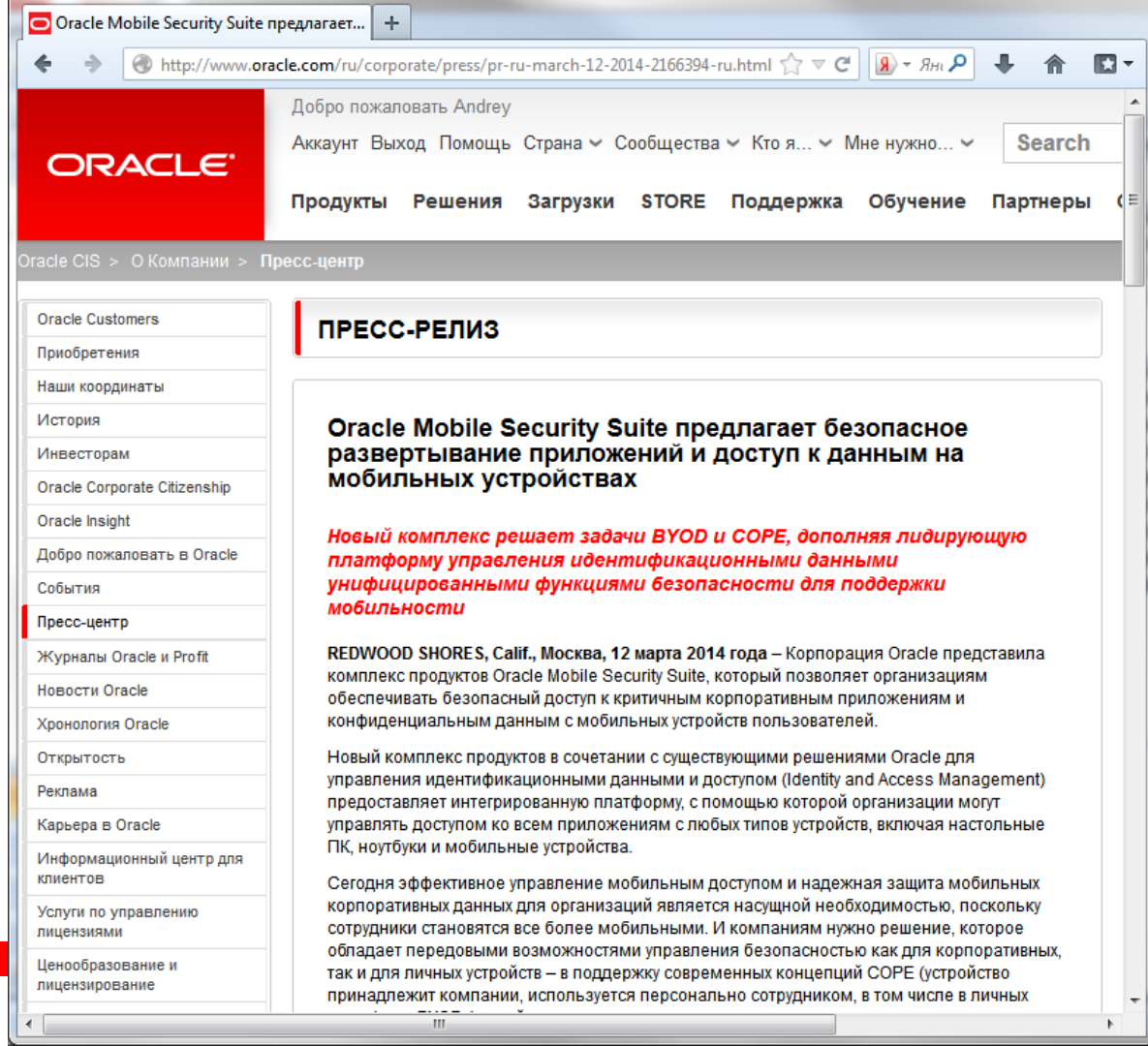


- Корпоративные политики безопасности не мешают персональному использованию устройства
- Защита корпоративной среды от проникновения угроз через мобильный VPN
- Набор защищенных мобильных приложений и средств контейнеризации

OMSS

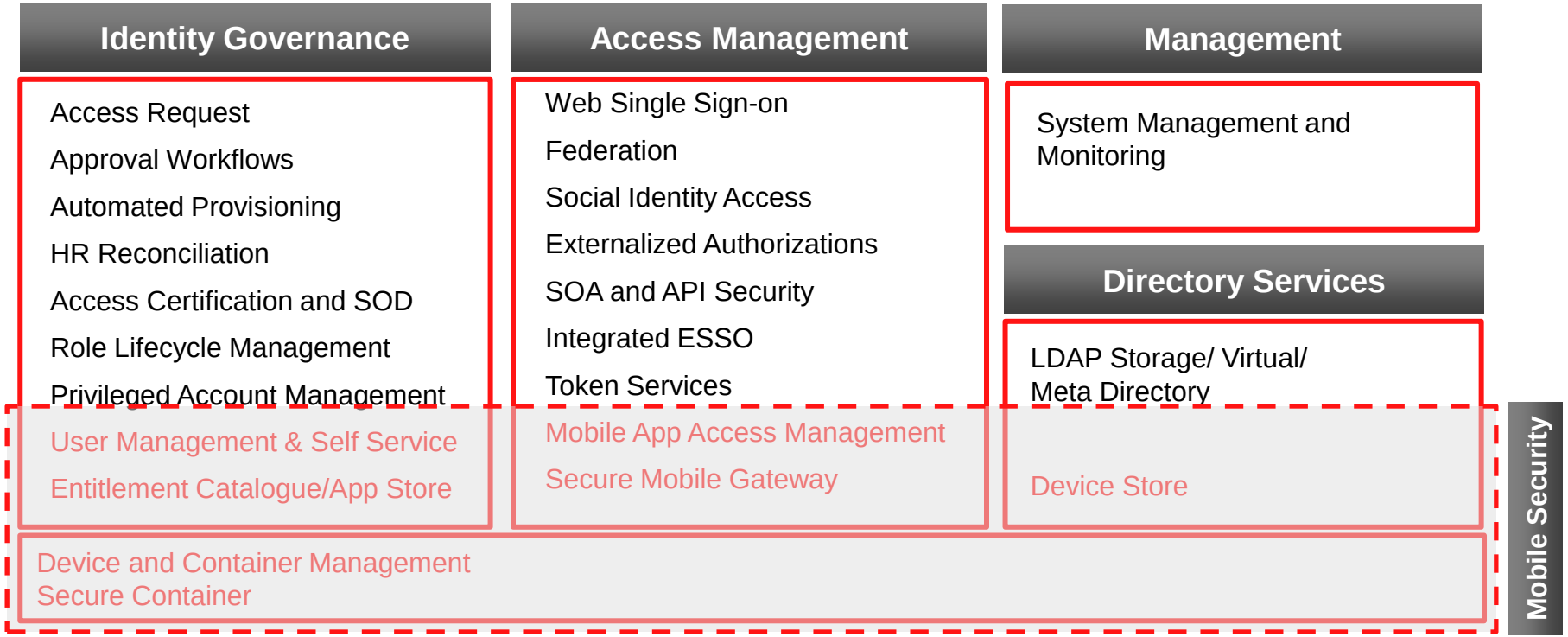
Расширение IdM-платформы Oracle, обеспечивающее безопасность мобильных корпоративных данных и приложений

В ближайших планах – интеграция со средой разработки мобильных приложений

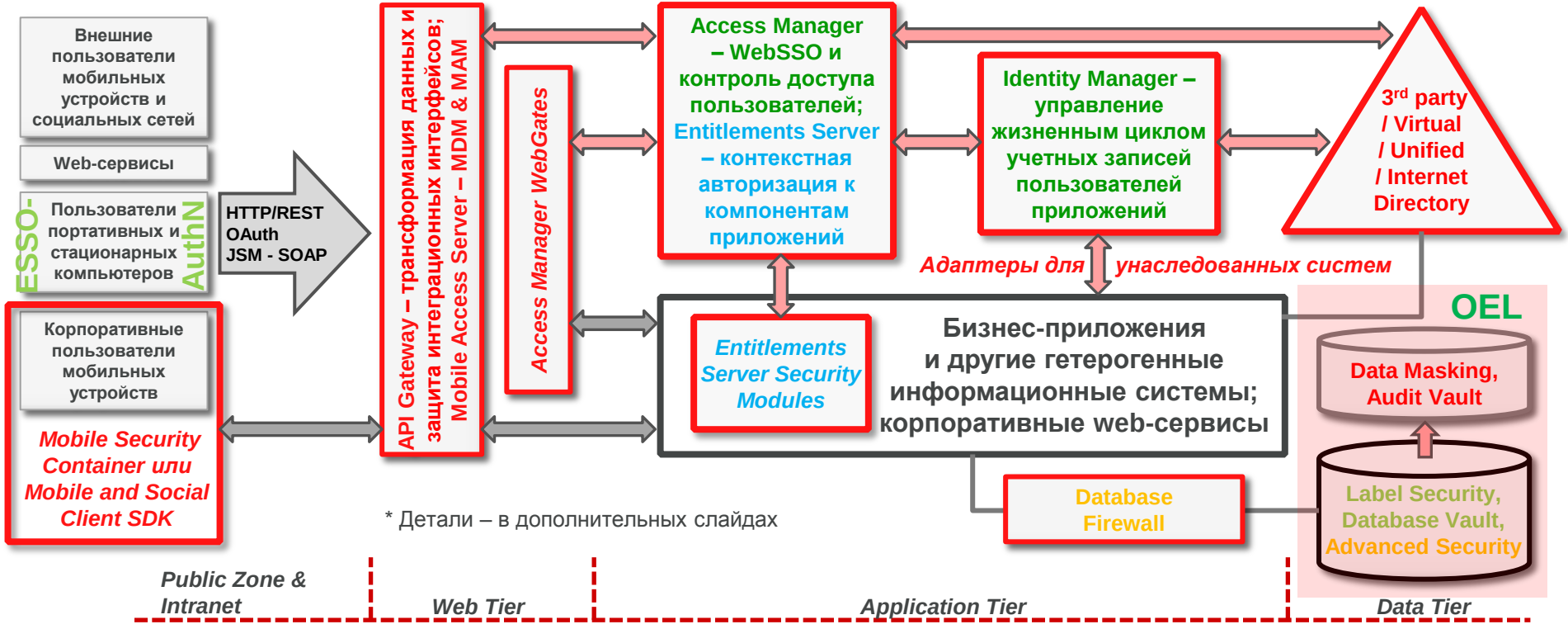


Oracle Identity Management 11g R2 PS2

Теперь охватывает мобильную среду



Рекомендуемые сертифицированные* решения безопасности Oracle



ORACLE IDM ОБЕСПЕЧИВАЕТ РЕАЛИЗАЦИЮ БИЗНЕС-ИНИЦИАТИВ И ВЫПОЛНЕНИЕ ЗАКОНОДАТЕЛЬНЫХ ТРЕБОВАНИЙ

Ваши инвестиции будут надежно защищены

Начните использование прямо сейчас!

Первоклассно!

Oracle Enterprise Security

- Полное и открытое решение
- Проверенное при многочисленных внедрениях
- Обеспечивающее надежную безопасность частным и публичным «облакам»
- Предлагающее сервис-ориентированную безопасность
- Доступное для проверки

Дополнительная информация

oracle.com/identity security-orcl.blogspot.ru

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

Внедрение средств защиты приложений в ЦОД

Database Security – core

- Label Security – для защиты строк таблиц за счет использования составных меток и меток безопасности, регулирующих права доступа для разных категорий пользователей; имеется серт. ФСТЭК
- Advanced Security – для защиты данных СУБД на дисках и в архивах (TDE) путем изменения формата хранения, а также – изменение способа отображения данных полей СУБД при запросах (Data Redaction); запланирована серт. ФСТЭК
- Database Vault – для защиты объектов СУБД и разграничения доступа к ним на основе политик; обеспечивает изоляцию бизнес-данных от администратора СУБД; имеется серт. ФСТЭК

Внедрение средств защиты приложений в ЦОД

Database Security – firewall, audit & masking

- Audit Vault and Database Firewall – для высокопроизводительного мониторинга SQL-трафика и реализации политик контроля доступа; обеспечивает защиту от SQL-инъекций и консолидацию данных аудита (базы данных, каталоги, операционные системы, пользовательские файлы); гетерогенное решение; запланирована серт. ФСТЭК
- Oracle Enterprise Manager Data Masking Pack – для создания тестовых баз данных заданного объема, используемых для разработки/тестирования приложений, путем замены конфиденциальных данных тестовыми значениями с сохранением типа данных и логической структуры БД в целом; гетерогенное решение

Внедрение средств защиты приложений в ЦОД

Database Security на доверенной операционной системе

- Средства защиты СУБД Oracle (например, DB Vault) может быть использованы для защиты ПДн 1-го и 2-го типов, если установить их на операционную систему Oracle Enterprise Linux, которая в соответствии с сертификатом №3095 сроком действия до 13 февраля 2017 г. соответствует требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 3 классу защищенности и «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 2 уровню контроля.

Внедрение средств защиты приложений в ЦОД

Identity Governance

- Обеспечивает консолидацию идентификационных данных и автоматизированное управление их жизненным циклом – заведение, изменение прав доступа, самообслуживание (например, смену паролей и формирование заявок), контроль изменений привилегий в подключенных системах, блокирование, удаление, историческую отчетность, документооборот по согласованию заявок, соответствие законодательным нормам (OIM); имеется серт. ФСТЭК с контролем НДВ
- Обеспечивает управление жизненным циклом ролей, их оптимизацию и согласование, а также – контроль операций, осуществляемых от имени суперпользователей (OIA&OPAM)

Внедрение средств защиты приложений в ЦОД

Directory Services & Access Management

- Обеспечивают стандартизацию форматов хранения и обработки идентификационных данных и их синхронизацию с помощью создания высокопроизводительных реальных и виртуальных LDAP-каталогов (ODS)
- Обеспечивает аутентификацию, WebSSO, авторизацию к запрашиваемым ресурсам, аудит запросов, передачу приложениям меток аутентификации, контроль сессий и таймаутов, перенаправление на сервис самообслуживания для смены/восстановления пароля (OAM); имеется серт. ФСТЭК с контролем НДВ

Внедрение средств защиты приложений в ЦОД

Access Management

- Обеспечивают распределенную контекстную авторизацию к сервисам, объектам приложений и СУБД на основе централизованно задаваемых политик и получение отсутствующих в запросе атрибутов из внешних источников (OES); идет серт. ФСТЭК с контролем НДВ
- Обеспечивает противодействие мошенническим действиям, выявляемым в реальном масштабе времени за счет комплексного анализа поведения пользователей и взаимодействия с ними по нескольким каналам данных (e-mail, SMS, чат и т.п.); предоставляет консоли для анализа инцидентов и аналитику для их расследования (OAAM)

Внедрение средств защиты приложений в ЦОД

Web Services Security & Access Management

- Обеспечивают применение политик доступа к Web-сервисам на периметре (API Gateway) и внутри его (Web Services Security); реализует защиту от таких внешних угроз, как подмена содержимого, вирусы, DDoS, XML-бомбы, SQL инъекции, межсайтовые скрипты, ведущие к недоступности сервисов, раскрытию конфиденциальной информации, ущербу на стороне клиента
- Интегрируется с системой определения политик Access Management, преобразует REST в SOAP и обратно на лету

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

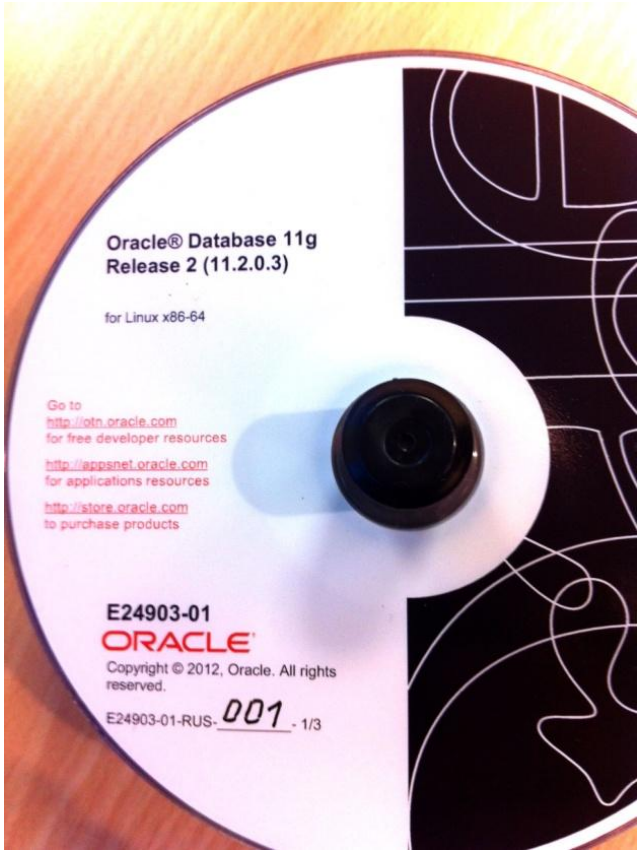
Система сертификации
№ РОСС RU.0001.01БИ00

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2238

Выдан 23 декабря 2010 г.
Действителен до 23 декабря 2013 г.
Срок действия продлен до 23 декабря 2016 г.

Настоящий сертификат удостоверяет, что **программное обеспечение Oracle Identity Access Management Suite 11g** (партия из 200 (двухсот) экземпляров продукции с серийными №№ с 0001 по 0200, маркированных знаками соответствия с № Г 617000 по № Г 617199) производства компании Oracle, Inc. является программным средством защиты информации, 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.



ORACLE