
ORACLE®

Республика Башкортостан
ДЦ «Юбилейный»
17–22 февраля 2014 года

ORACLE

Решения Oracle по защите информации

Сергей Базылько, к.ф.-м.н.
Менеджер по продажам продуктов безопасности

Тенденции

- Безопасность – как двигатель прогресса
  - От стоимости ведения бизнеса – к платформе для предоставления новых услуг
- Nexus - силы
  - Мобильность, облака, социальные сети, интернет вещей
- Кибербезопасность
  - Advanced Persistent Threats

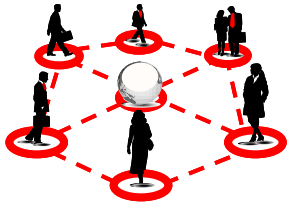
Nexus Forces

Mobile

- BYOD усложняет защиту ПДн
- Разграничить личные и корпоративные данные
- Низкая защищенность устройств и приложений

Cloud

- Приложения: собственные, в частном или публичном облаке
- Учетные записи для SaaS
- Портал доступа как облачная услуга



Social

- Пользователи хотят использовать социальные аккаунты
- Упрощение регистраций и маркетинга
- Открытые стандарты OAuth & OpenID

Internet of Things

- Миллиарды подсоединенных устройств
- Генерирует много данных
- Нужно управление политиками в реальном времени, безопасность и управление жизненным циклом

Взрывной рост учетных данных

Восстание машин

Людей на Земле

8.3 Млрд.

К 2050г.

Скорость роста

1.1%

Oracle case study 2013

Облачных серверов

847 Млн.

К 2016г.

Скорость роста

35%

IHS Research 2012

Интернет вещей

50 Млрд.

К 2020г.

УДВОЕНИЕ

каждые 2 года

CISCO IBSG 2012

Oracle Identity Governance

Платформа для управления распределением прав и полномочий

Пакет решений для управления доступом

Полный. Современный. Интегрированный.

ORACLE SIEBEL PeopleSoft. SAP JDEDWARDS другие…

Управление идентификацией
Identity Governance

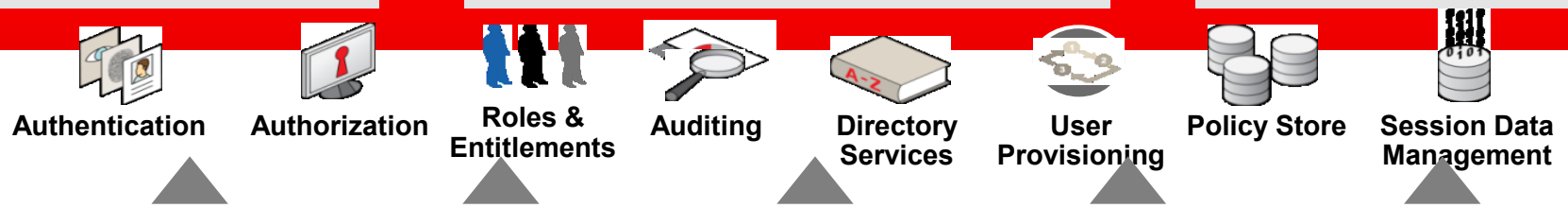
- Жизненный цикл учетных записей
- Ролевое управление
- Аналитика, проверка политик
- Анализ рисков
- Привилегированный доступ
- Управление мобильными приложениями

Управление доступом
Access Management

- Single Sign-On & Federation
- Безопасность Web сервисов
- Аутентификация
- Авторизация и назначение прав
- Доступ мобильных устройств и приложений

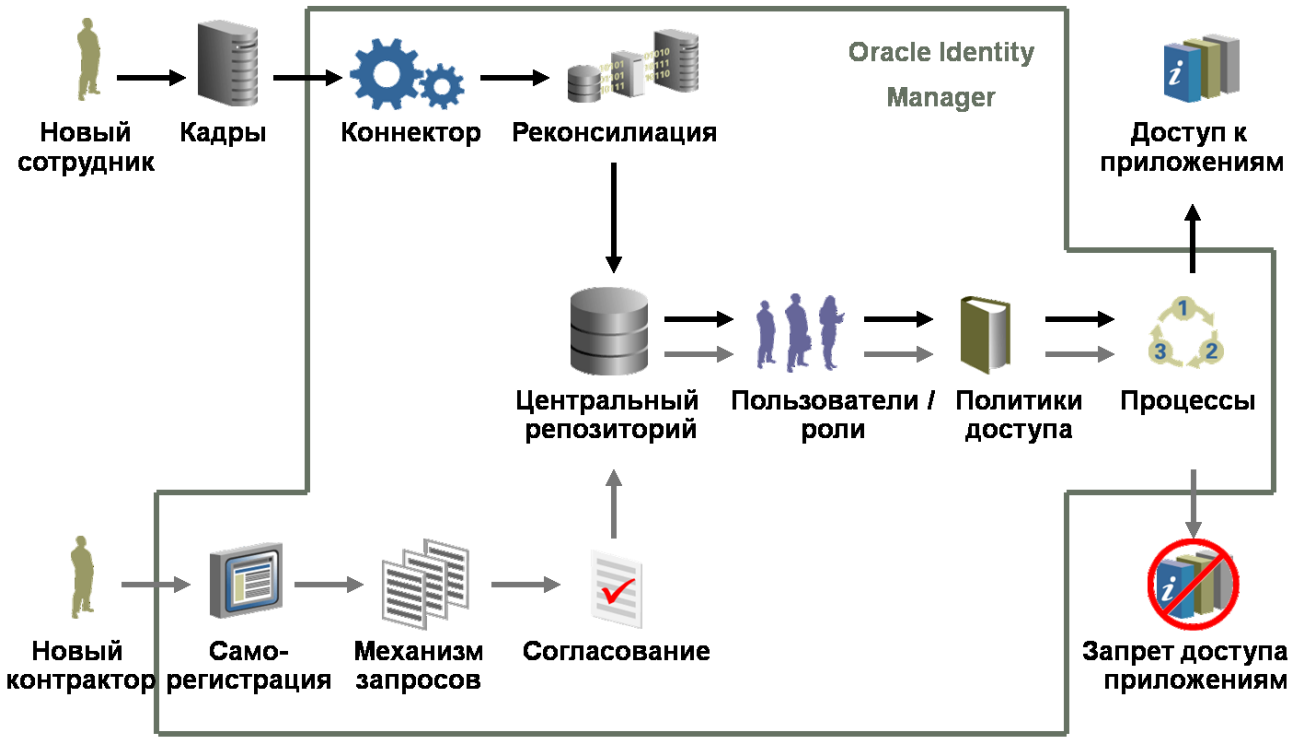
Сервисы директории
Directory Services

- LDAP хранилище
- Виртуальное хранилище
- Синхронизация LDAP



Управление учетными записями

- Oracle Identity Manager как первый шаг реализации программы защиты доступа

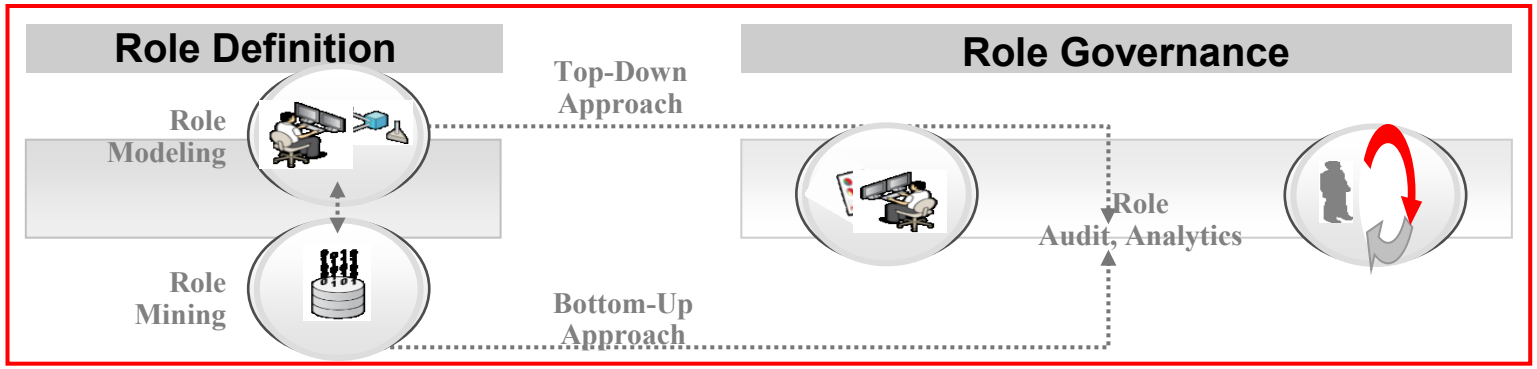


Платформа для управления идентификационными данными

- Oracle **Identity Governance Suite** – следующий этап развития системы управления учетными записями

Oracle Identity Governance

Управление жизненным циклом ролей



Изменения

- Согласования изменения ролей
- Версионность и откат
- Возможность сравнения и отката
- Анализ влияния изменений

Аудит

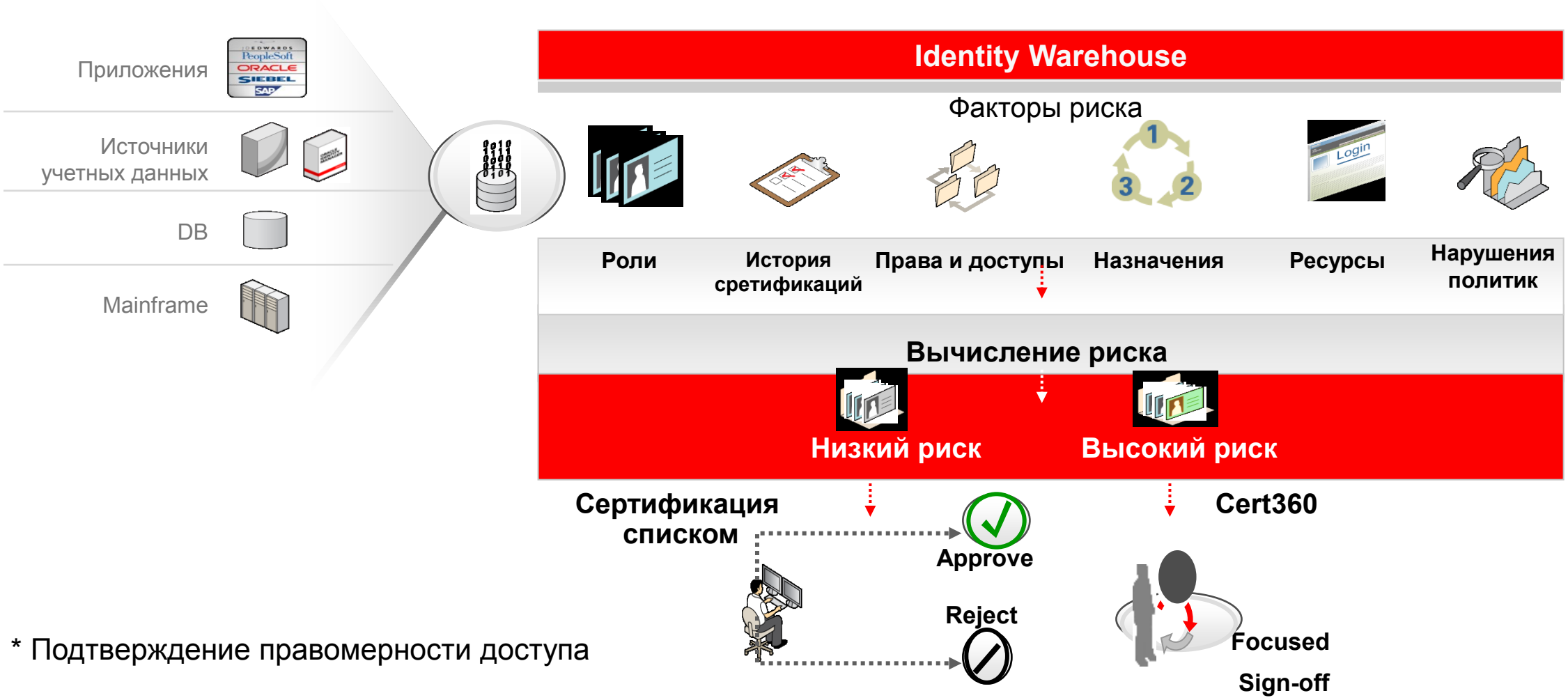
- История соответствия ролей и доступов
- История членства в ролях
- История согласований
- История владельцев ролей

Управление

- Аттестация определения роли
- Аттестация членства в роли
- Консолидация ролей
- Role Mining

Oracle Identity Governance

Сертификация* с учетом риска

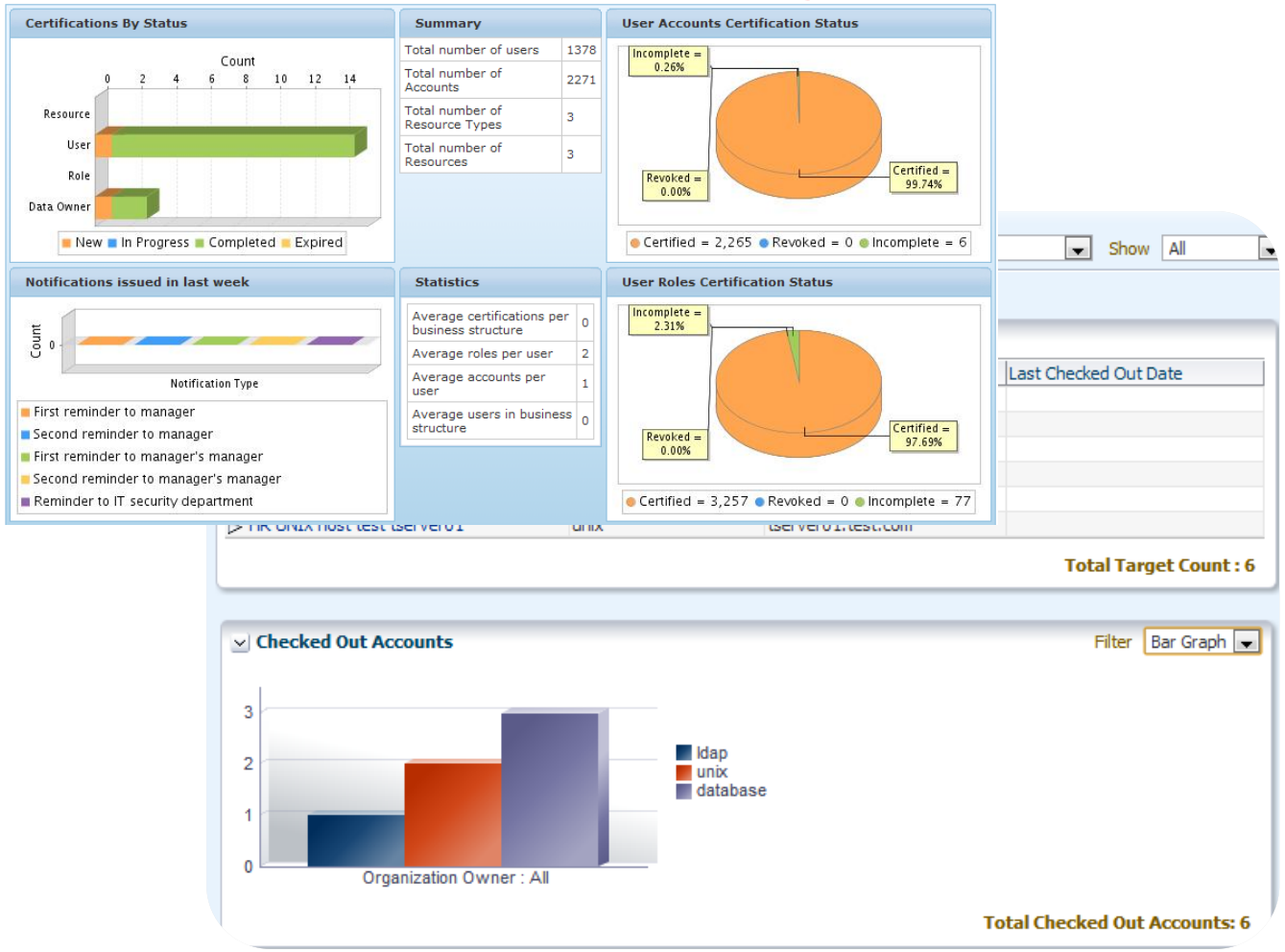


* Подтверждение правомерности доступа

Oracle Identity Governance

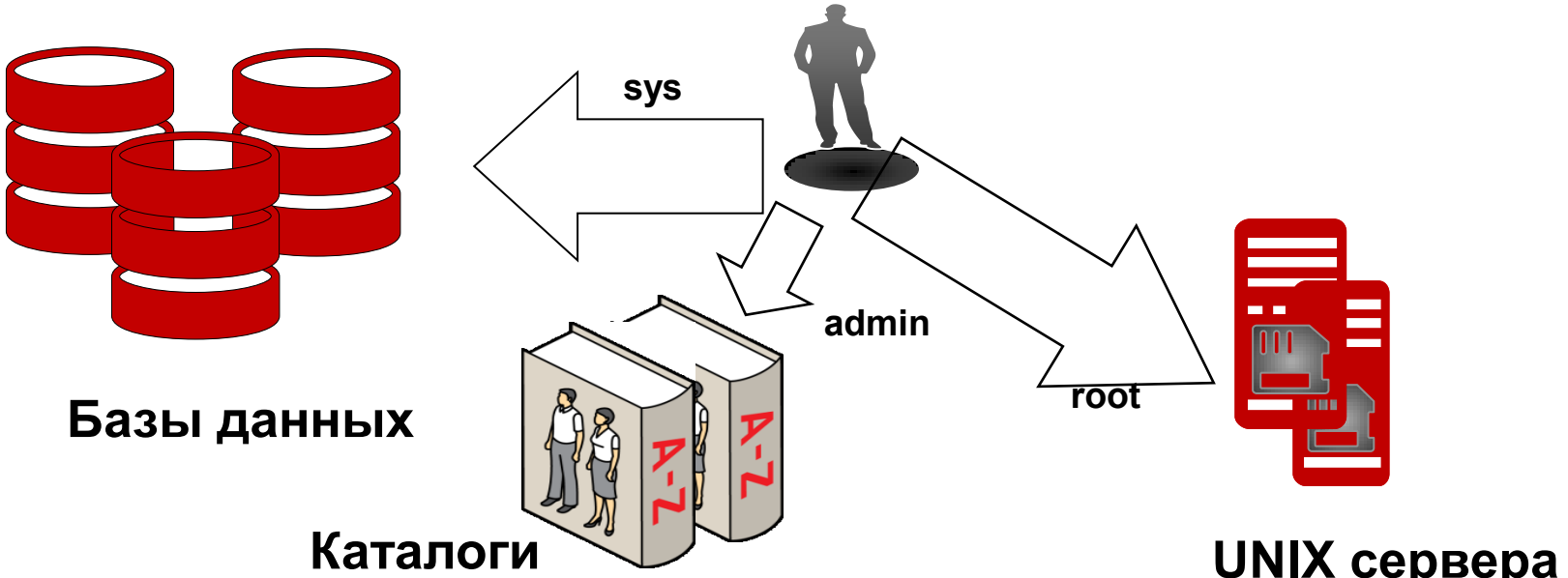
Отчетность и аудит предоставления доступа

- Интерактивные отчеты для анализа рисков
- Более 80 отчетов для всестороннего рассмотрения доступа пользователей
- Различные возможности по установке, отчетность по расписанию
- Открытая схема данных



Oracle Identity Governance

Контроль и прозрачность предоставления административного доступа

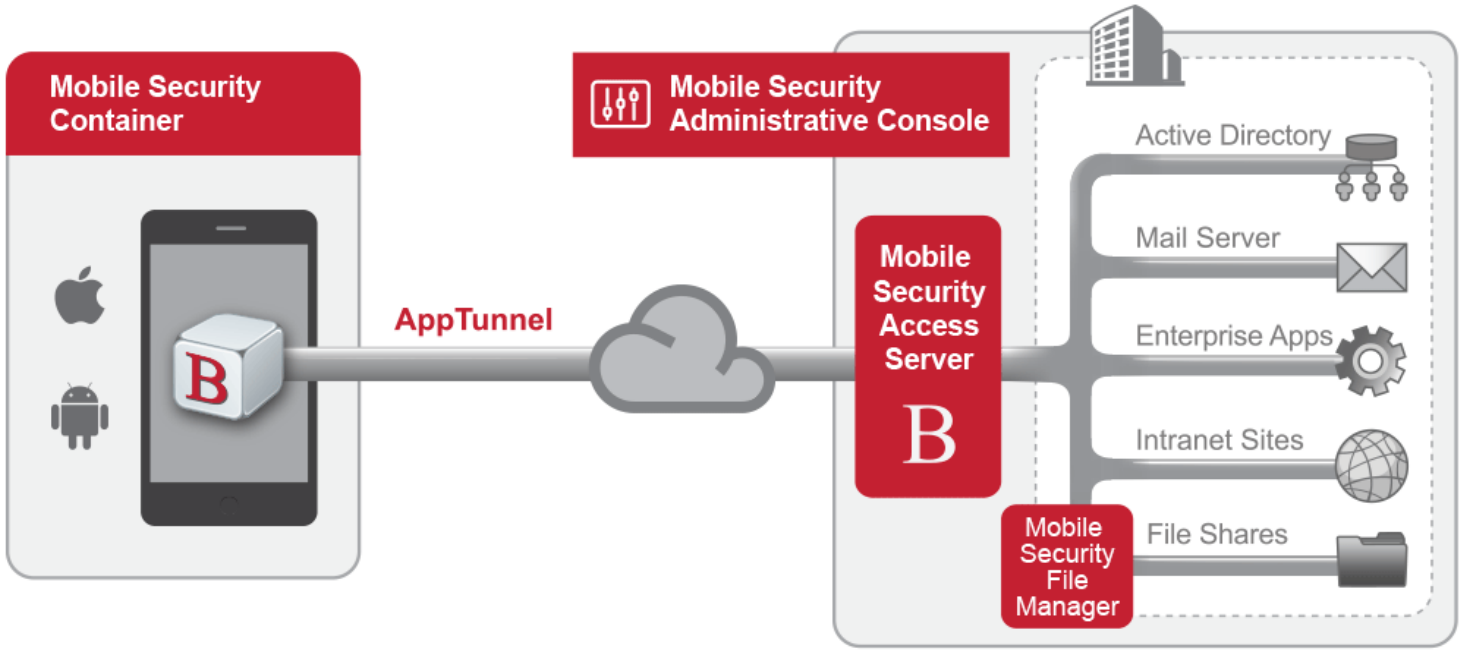


- Привилегированные учетными записи – ключевая «точка входа» для мошенников
- Сложность мониторинга использования разделяемых среди нескольких администраторов учетных записей
- Избыточные права доступа – главное направление в атаках на базы данных

Oracle Identity Governance

Управление мобильными приложениями

- Защищенный изолированный контейнер на устройстве пользователя
- Управление приложениями, доступными в контейнере



Преимущества Oracle Identity Governance

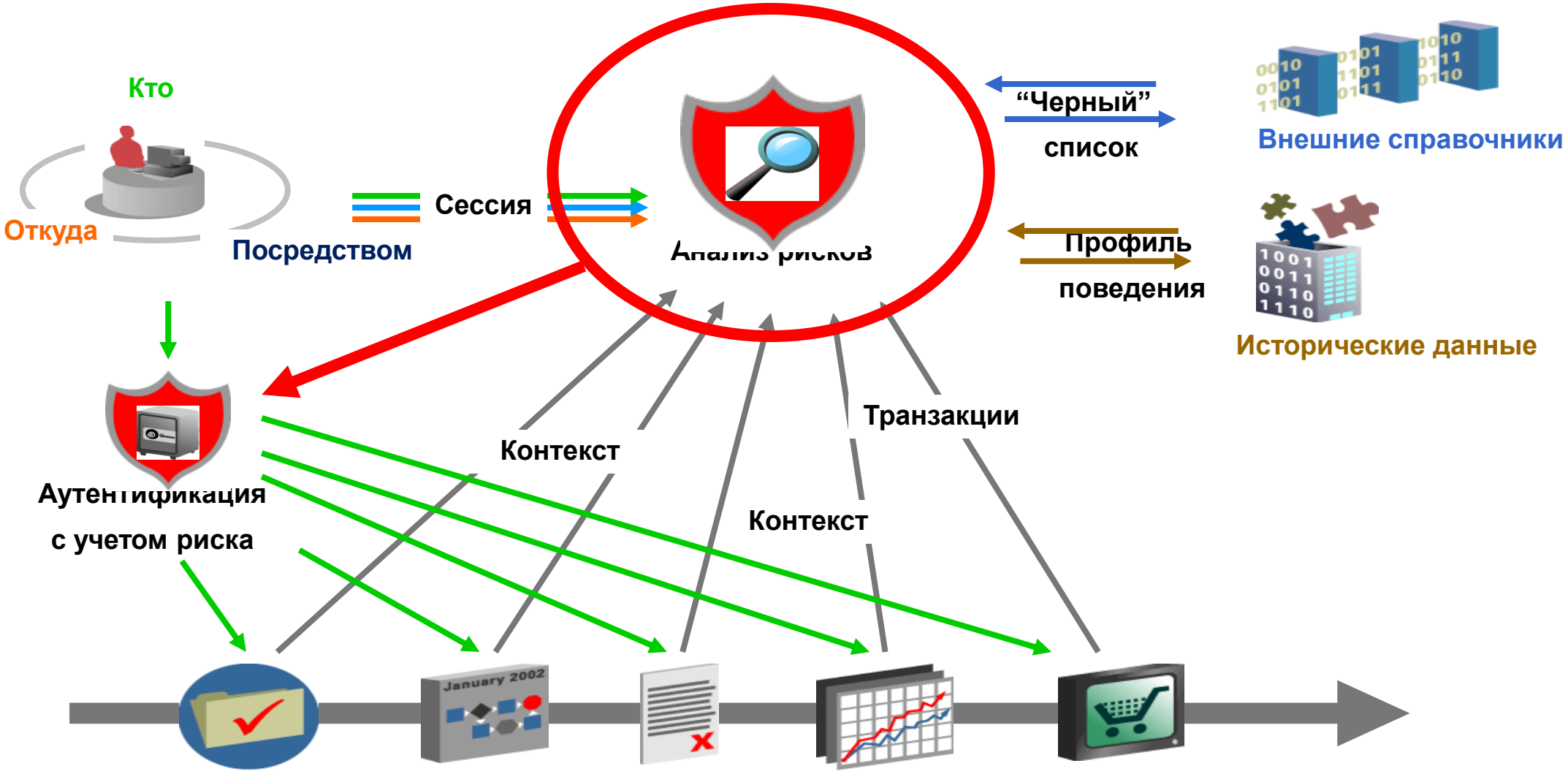
- Соответствие требованиям законодательства
  - Аудит и анализ использования доступа в информационно-управляющие системы (ИУС)
  - Наличие сертификата ФСТЭК
- Повышение уровня информационной безопасности и снижение рисков
  - Минимизация необходимых прав, предоставляемых сотрудникам
  - Снижение риска конфликта интересов в правах и возникновения несовместимых полномочий
  - Исключение возможности несанкционированного и/или бесконтрольного использования привилегированных учетных записей
- Снижение расходов на обслуживание
  - Перенос функции проверки правомочности предоставленных доступов на владельцев ИУС
  - Автоматическое удаление неподтвержденных доступов
- Повышение производительности
  - Ускорение и упрощение процедур подтверждения руководством доступа своих сотрудников
  - Стандартизация процедур подтверждения доступов для всех ИУС
  - Увеличение ответственности владельцев ИУС

Авторизация с учетом риска

Oracle Adaptive Access Manager

- Имя пользователя и пароль верны, но действительно ли это “наш” пользователь (параметры устройства, геолокационные данные)?
- Делает ли клиент, что-нибудь подозрительное (политики и профиль) ?
- Проходит ли дополнительную проверку, если уровень риска проведения транзакции высокий?

Схема работы



Сбор параметров устройств

Логика определения уникальности: внутренний алгоритм OAAM 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.

Мобильные устройства +: информация о характеристиках у-ва и другие данные

Повторная аутентификация: сбор характеристик устройств повторяется в течении сессии не однократно для предотвращения его подмены.

Oracle Mobile Security

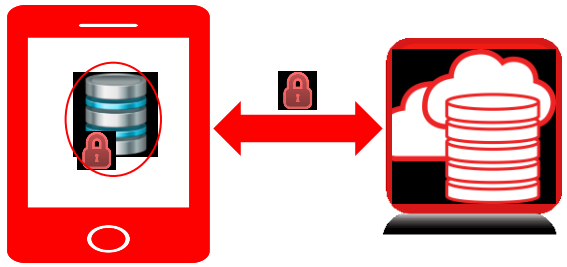
Oracle Mobile Security

Защита и управление корпоративными приложениями и данными на устройствах

Защищенный контейнер для защиты приложений

- Политики, контролирующие перемещение данных в/из контейнера
- Разграничение, защита и стирание корпоративных приложений и данных
- Универсальных подход для всех платформ

Защищенное управление и контроль за корпоративными приложениями



- Защищенная связь с корпоративными серверами приложений
- Корпоративный магазин приложений

Использование существующей IDM-платформы

- Управление пользователями и устройствами
- Общие пользователи, роли, политики, запрос доступа, сертификация, и т.д.
- SSO для нативных и браузерных приложений
- Рискоориентированный подход к авторизации

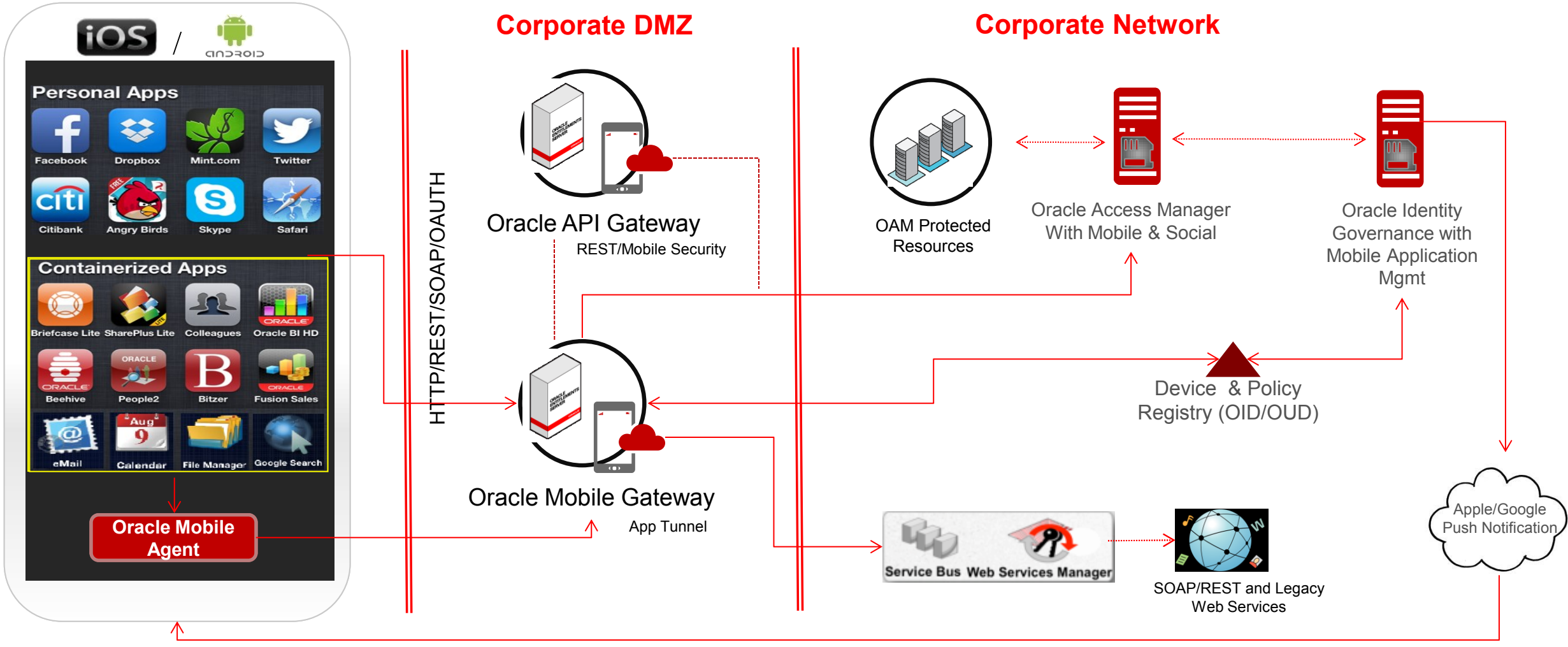
Oracle Mobile Security Vision

Реализация требований заказчиков к решениям Mobile Security

- Mobile Security Suite расширяет платформу Oracle IDM для управления контейнерами и приложениями
- Разграничение личных и корпоративных данных и приложений
- Защита приложений не влияет на остальные функции устройства
- Расширяет платформу управления доступом (Access Management) возможностями управлять доступом с устройств/приложений
- Приложения на Oracle/ADF Mobile изначально безопасны с использованием сервисов безопасности

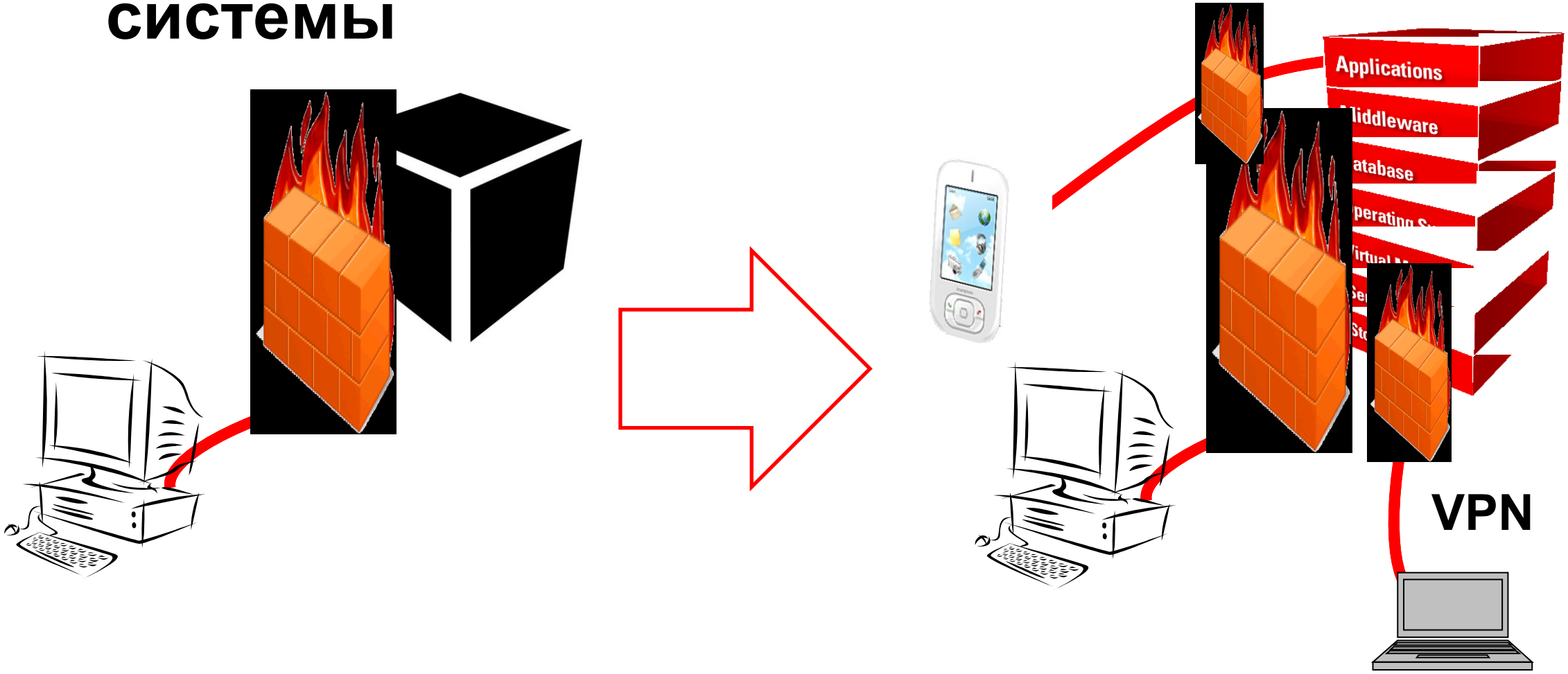
Oracle Mobile Security Suite

Архитектура



Защита баз данных

Новый взгляд на информационные системы



Риски данным на уровне базы

- Доступ с административными привилегиями
  - На уровне операционной системы
  - На уровне базы данных
- Доступ к данным в различных средах
  - Среды разработки и тестирования
  - Бэкапирование
  - Продуктивные среды

Решения по защите баз данных

Security inside out

- В базах данных ORACLE
  - Шифрование данных при хранении, передаче и архивации
  - Проверка данных пользователя
  - Контроль доступа привилегированных пользователей
  - Многофакторная авторизация
  - Контроль защищенности рабочего окружения продуктивных СУБД
  - Reduction – модификация данных в ответе базы
- В гетерогенных средах
  - Аудит активности и отчетность
  - Мониторинг трафика и защита базы данных от нежелательной активности
  - Маскирование критичных данных в тестовых средах

Oracle Database Security

Разработка

Тестирование

LAST_NAME	SALARY
Иванов1	54,321
Иванов2	12,345

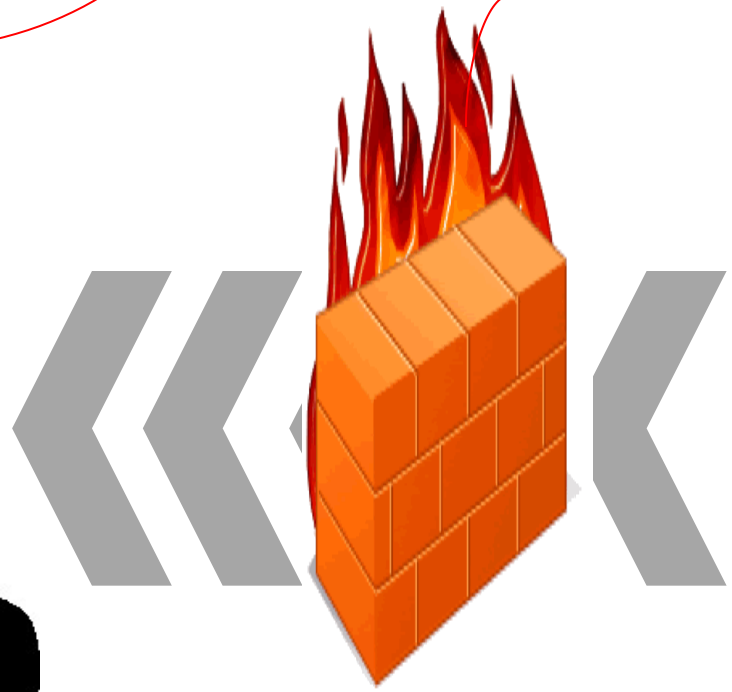
Data Masking

LAST_NAME	SALARY
Иванов	40,000
Петров	60,000

ODV

audit.log

AVDF



Secure Backup

AS

Преимущества Oracle DB Security

Повышение уровня информационной безопасности

- Реализация принципа разделения полномочий
  - Контроль доступа пользователей ОС серверного оборудования к данным в базах
  - Контроль доступа администраторов БД к закрытым областям
    - Усиление контроля над исполнением критичных операций
  - Контролируемый доступ к резервным копиям
- Обеспечение полноты аудита
  - Консолидация аудита доступа как по ИУС так и по каналам (SQL-трафик, аудит БД, логи ОС)
- Предотвращение утечек через среды тестирования/разработки
- Выполнение требований законодательства в части обеспечения конфиденциальности данных
  - Сертификат ФСТЭК 2858 на Oracle DB с опцией Database Vault

Преимущества Oracle DB Security

Снижение затрат

- Ускорение сбора информации о фактах доступа к критичным/конфиденциальным данным
- Низкие затраты на изменение инфраструктуры для обеспечения мониторинга
- Снижение нагрузки на базы данных за счет использования внешнего хранилища аудит-логов
- Автоматизация процедур обезличивания данных при передачи в тестирование/разработку
- Оптимизация затрат на тестирование
- Усиление механизмов защиты ИУС без внесения изменений в приложения

Спасибо за внимание!

Сергей Базылько, к.ф.-м.н.

Менеджер по продажам продуктов безопасности

sergey.bazylko@oracle.com

+7 915 018 8804

ORACLE IS THE INFORMATION COMPANY