

ORACLE®

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Облачные решения Oracle

Вопросы соблюдения
законодательства в области
защиты персональных данных



Андрей Гусаков,
руководитель группы консультантов по Enterprise Security

Москва, май 2015 года

Аналитики о мировом рынке облачных вычислений



**Облачные вычисления
– признанный тренд**

84%

- Using Cloud today or will be in Two Years



**Взрывной рост
использования SaaS**

\$56_B

- Total spending on SaaS by 2018 at 20% CAGR



**Увеличение
интереса к PaaS**

~90%

- Will adopt PaaS within Five Years @ 22% CAGR

* CAGR - Compound Annual Growth Rate/Совокупный среднегодовой темп роста

Oracle помогает добиться успеха в цифровом мире



СОВРЕМЕННЫЙ БИЗНЕС

Рекомендации по каждой
функции, выполняемой на
предприятии



СОВРЕМЕННЫЕ РЕШЕНИЯ

Персонализированные,
интегрированные и
безопасные



ПРАКТИЧНЫЙ ПУТЬ

для достижения
поставленных бизнес-
целей

Пресс-релиз

Oracle добавляет новые сервисы к наиболее полному в мире корпоративному облачному портфолио

Выпуск большого числа новых платформенных и инфраструктурных сервисов поможет разработчикам, ИТ-специалистам и бизнес-пользователям проводить технологические преобразования и ускорять инновации в бизнесе.

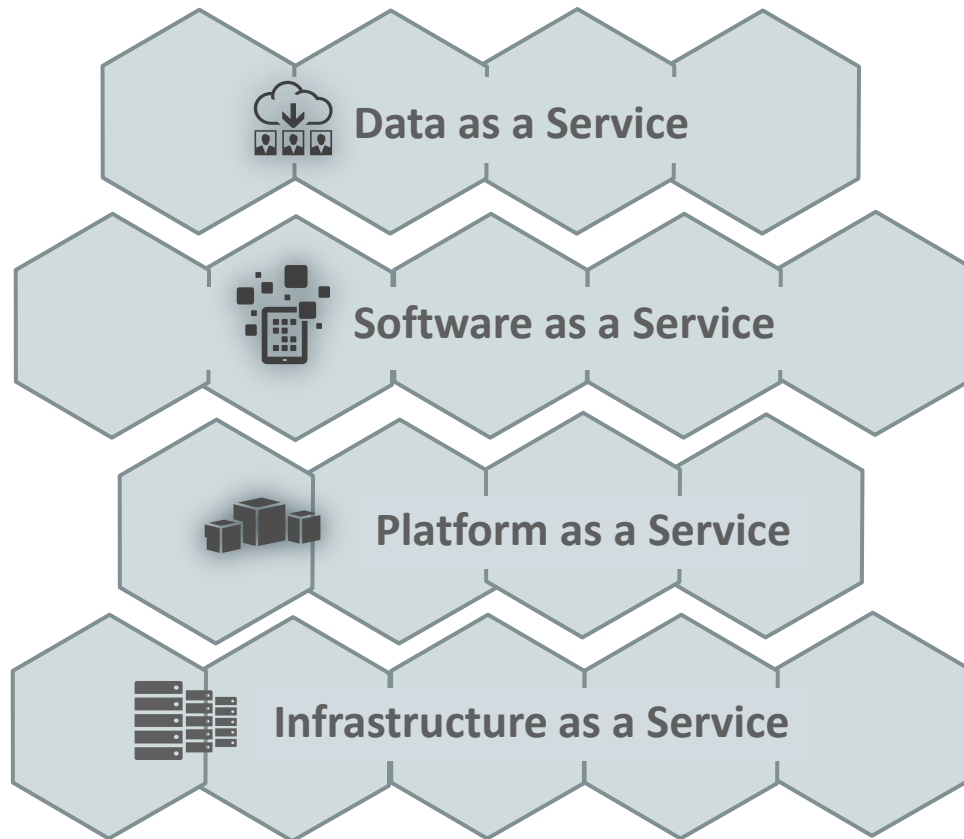
Redwood Shores, California, Москва—23 Июнь 2015 г.



«Oracle растет очень быстро. За последний квартал мы продали SaaS- и PaaS-решений на \$426 миллионов. Это рост на 200% по сравнению с тем же кварталом прошлого года. Это рекорд в индустрии, ни одной компании еще не удавалось продать столько за один квартал», — заявил Эллисон. — Oracle - единственная компания на планете, способная предоставить полный, интегрированный и основанный на стандартах комплекс облачных сервисов на каждом уровне облака. Такие технологические преимущества позволяют нам быть намного более рентабельными по сравнению с конкурентами.»

oracle.com/ru/corporate/pressrelease/comprehensive-cloud-platform-20150622.html

Стратегия Oracle в области облачных вычислений

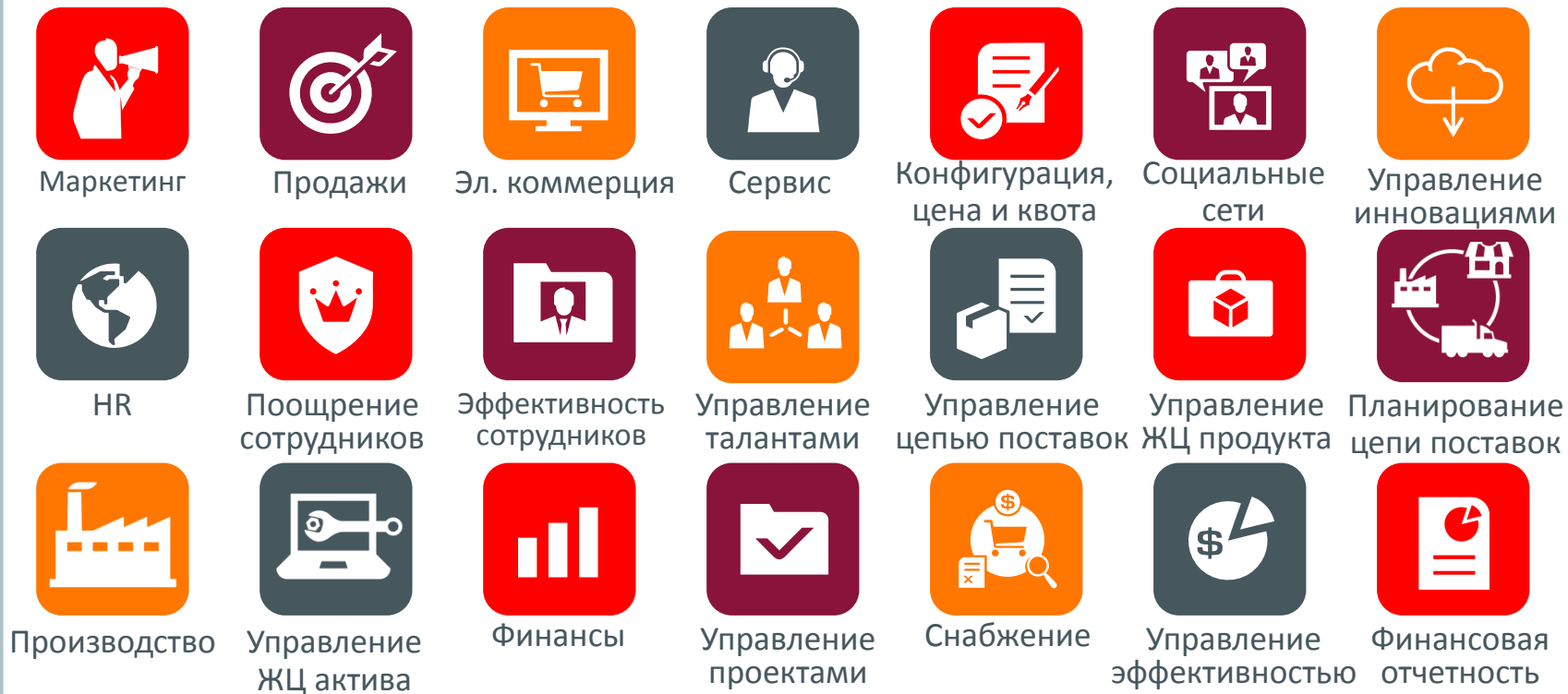


Предоставление лидирующих технологий Oracle в области ПО заказчикам и партнерам во всем мире через Интернет



Oracle Applications – Полный портфель решений поддержки современного цифрового бизнеса

БИЗНЕС ПРИЛОЖЕНИЯ



Платформа и инфраструктура

CX
платформа

HCM
платформа

ERP
платформа

SCM
платформа

EPM
платформа

Автоматизация всех бизнес-взаимодействий.

1 — Унификация процессов, данных, контролей доступа и бизнес-аналитики

2 — Модульный дизайн и изменения со скоростью роста бизнеса

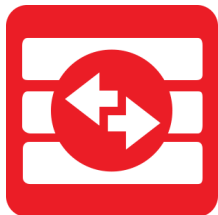
3 — **18 лидеров** в своих категориях

4 — Встроенная аналитика, возможности социального взаимодействия и мобильность

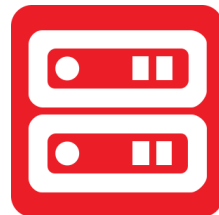
5 — Стандартизация на современной платформе приложений

6 — PaaS для повышения эксплуатационных характеристик приложений

Публичные сервисы Oracle IaaS & PaaS для бизнес-пользователей, разработчиков и IT-подразделений



Storage



Compute



Messaging



Secure Identity

Coming Soon



Documents



Social Network



Business Intelligence



BPM



BigData

Coming Soon



Node.js

Coming Soon



Database



Database Backup



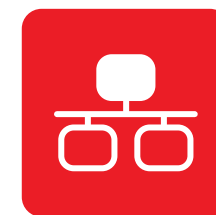
Java



Developer

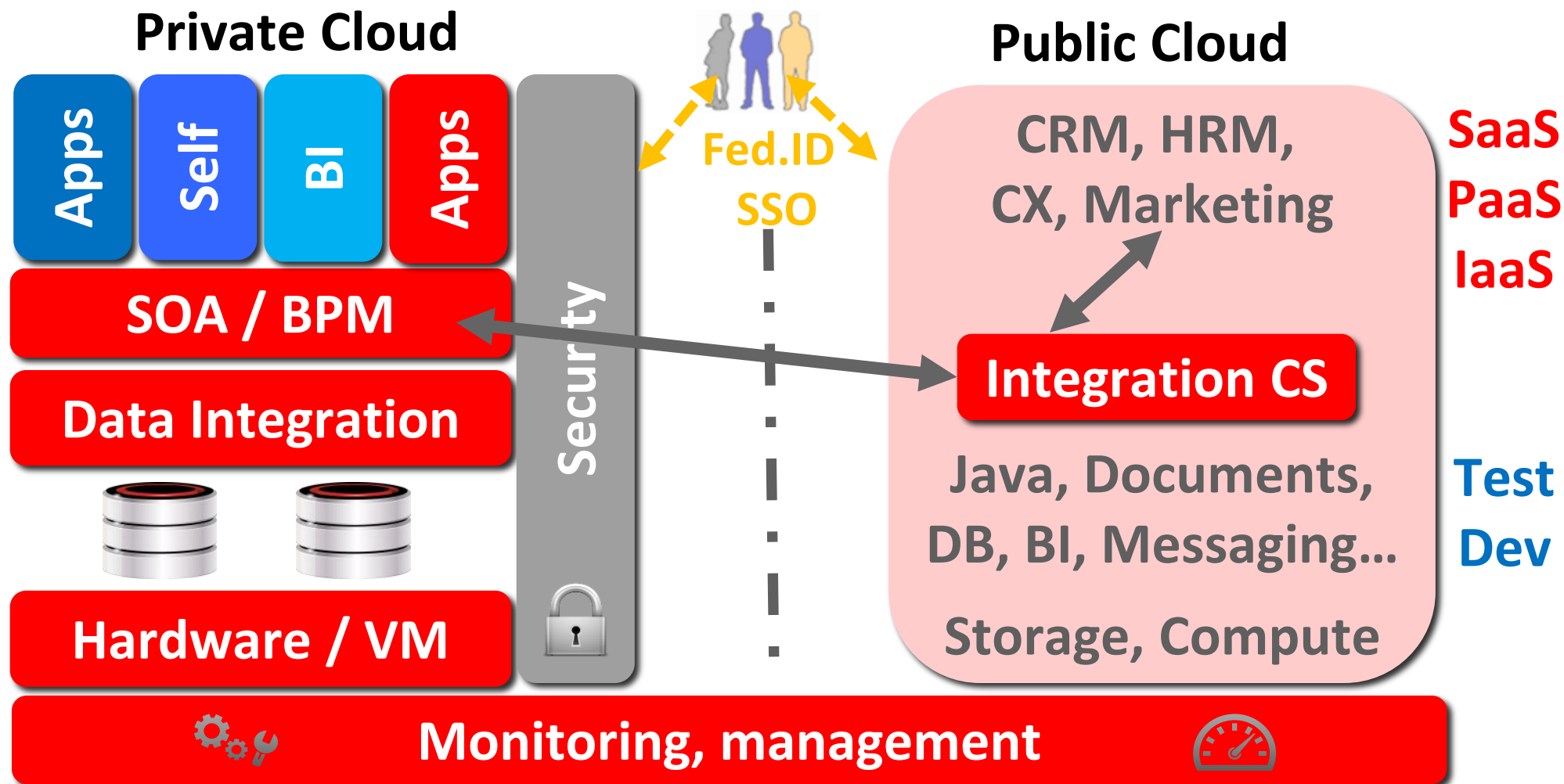


Mobile

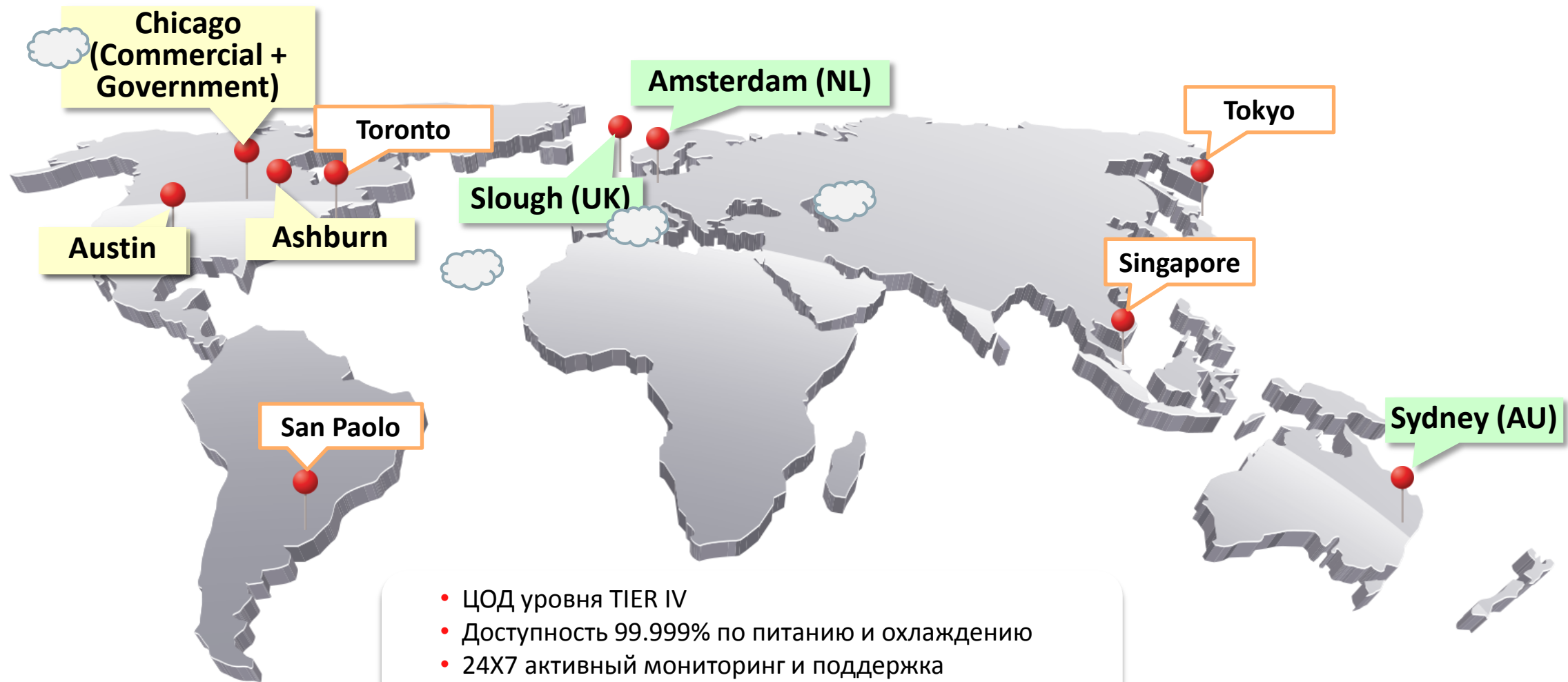


Integration

Пример интеграции и кастомизации публичных облачных сервисов в гибридном облаке



Собственные ЦОДы Oracle, предоставляющие публичные облачные услуги (IaaS+PaaS+SaaS)



- ЦОД уровня TIER IV
- Доступность 99.999% по питанию и охлаждению
- 24X7 активный мониторинг и поддержка
- Независимый по отношению к телеком провайдерам

Защита информации... юридически

Разделы Oracle Cloud Security Policy

1. User Encryption for External Connections
2. Network Access Control
3. Network Bandwidth and Latency
4. Anti-Virus Controls
5. Firewalls
6. System Hardening
7. Physical Security Safeguards
8. System Access Control & Password Management
9. Review of Access Rights
10. Security-Related Maintenance
11. Data Management / Protection
 1. Physical Media in Transit
 2. Data Disposal
 3. Security Incident Response
 4. Data Privacy

Source: «Oracle Cloud Hosting and Delivery Policies»

oracle.com/us/corporate/contracts/cloud-hosting-delivery-policies-1881437.pdf

Защита информации... юридически



- Сертификация Safe Harbour является обязательной для юрисдикции Европы (например: EU Directive 95/46/EC on Personal Data Protection, и т.д.)
- Oracle следует политике защиты данных Oracle's Services Privacy Policy:
<http://www.oracle.com/us/legal/privacy/services-privacy-policy/index.html>
- Oracle следует политике Data Processing Agreement для сервисов в Облаке Oracle:
<http://www.oracle.com/us/corporate/contracts/cloud-dpa-1014-2346862.pdf>

Organization Information:

Oracle America, Inc.
500 Oracle Parkway
Redwood Shores, California- 94065
Phone: 650-506-7000
Fax: 650-506-7200
<http://www.oracle.com>

Organization Contact:

Contact Office: Legal Department
Name: Alexis Goltra , Chief Privacy Officer
Phone: 781-744-0837
Fax: 781-744-0837
Email: alexis.goltra@oracle.com

Corporate Officer:

Corporate Officer: Alexis Goltra , Chief Privacy Officer
Phone: 781-744-0837
Fax: 781-744-0837
Email: alexis.goltra@oracle.com

Safe Harbor Information:

Certification Status: Current
Original Certification: 4/18/2002
Next Certification: 4/18/2015

Personal Information Received from the EU/EEA and/or Switzerland:

Personal information collected online and offline in connection with Oracle's business activities, including information concerning current, prospective and former: customers; suppliers and vendors; partners; employees; and in connection with services to Oracle's customers, access to information concerning our customers' customers and prospects, suppliers, vendors, partners and employees. In each case above, the data may include information obtained in connection with merger and acquisition activity, where it may be used for evaluation and integration purposes and for ongoing business management as outlined below. Oracle receives information from the EU and Switzerland concerning prospective, current and former employees, consultants, contractors and job applicants for processing and storage. Oracle collects, transfers, and uses this data for purposes of employee benefits and workforce management. This includes evaluation of qualifications for employment, provision of employment benefits, reporting, security management, administration of compensation, performance management and training, workforce management, budgeting and salary administration, business contact directory, company network access, authentication, personalization and legal compliance. Oracle maintains separate privacy policies for treatment of employee data and applicant data. Oracle receives information concerning customers, prospects, partners, vendors and suppliers. Oracle collects, transfers, and uses this information for a range of business purposes, including marketing and sales, provision of products and services, partner and supply chain management and legal compliance. Oracle maintains a privacy policy for information it collects in connection with its online and offline business activities. In other areas, such as the provision of hardware and software consulting, support, and On Demand/Cloud and other outsourcing services, Oracle acts as a data processor. When conducting those activities, Oracle holds and/or processes data at the direction of its customer, which acts as a data controller and is responsible for providing notices to and obtaining required consents from data subjects. Oracle does not control this data and any access to or use of such data is incidental to completing its contractual requirements for the customer. Oracle maintains a privacy policy in connection with its provision of services to its customers. For clarity, Oracle's Safe Harbor certification applies equally to the operations of companies Oracle has acquired over time, such as Peoplesoft, Siebel, Taleo, RightNow and ATG.

Privacy Policy Effective: 2/24/2014

Location: <http://www.oracle.com/html/privacy.html>

Regulated By: Federal Trade Commission

Privacy Programs:
TRUSTe

Verification: TRUSTe

Dispute Resolution:
TRUSTe Dispute Resolution Program); EU Data Protection Authorities (DPAs) Panel (for Human Resources Data Only; Federal Data Protection and Information Commissioner for Switzerland (FDPIIC) - HR Only

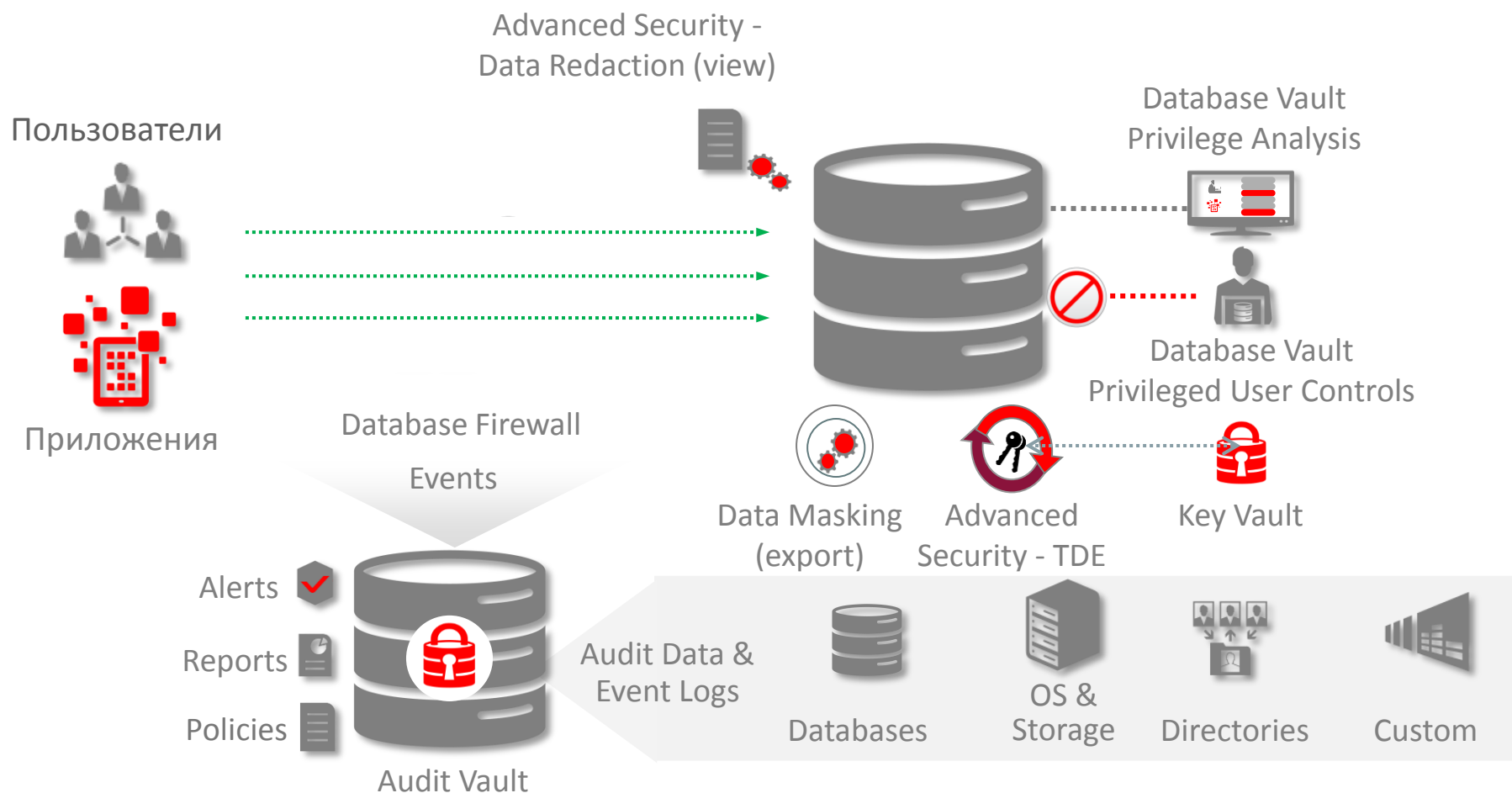
Personal Data Covered: Online and Offline Human Resources, Customer, Prospect, Partner, Supplier data; Services Data
Organization Human Resource Data Covered: Yes
Agrees to Cooperate and Comply with the EU and/or Swiss Data Protection Authorities: Yes

Relevant Countries from which Personal Information is Received:
Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom

Industry Sectors:
Computer Services - (CSV)

Защита информации... практически

Oracle Maximum Security Architecture



Защита информации... практически

- Персональные данные и другая критичная информация в Публичном Облаке Oracle защищена от неавторизованного доступа к файловой системе с помощью шифрования, прозрачного для приложений
- «All data stored in the Oracle Database Cloud - Multitenant Edition benefits from the use of Transparent Data Encryption. TDE encrypts data stored on disk and in backups, protecting against unauthorized direct file access»
https://cloud.oracle.com/downloads/WhitePaper_Database_4/Security+and+the+Oracle+Database+Cloud+Service.pdf
- Заказчики High Performance & Extreme Performance сервисов дополнительно могут использовать Label Security, Database Vault и Data Masking & Subsetting Pack
- <https://cloud.oracle.com/database?tabID=1406491812773>

Предложения Oracle по вопросам соблюдения законодательства РФ в области защиты персональных данных

Несколько юридических тонкостей – 1

Выдержки из Статьи 3 Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных"

Основные понятия, используемые в настоящем Федеральном законе:

- (3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая **сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение** персональных данных;
- (11) **трансграничная передача** персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

http://www.consultant.ru/document/cons_doc_LAW_166051/?frame=2

Несколько юридических тонкостей – 2

Выдержки из Статьи 12 Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных"

- (1) Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим ФЗ...

http://www.consultant.ru/document/cons_doc_law_166051/?frame=11

NB – В числе стран, которые ратифицировали Европейскую конвенцию о защите персональных данных ETS N 108

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?cl=rus&nt=108>

и стран, обеспечивающих адекватную защиту прав субъектов персональных данных (см. Приказ Роскомнадзора от 15 марта 2013 г. №274)

<http://www.rg.ru/printable/2013/04/26/perechen-dok.html>

перечислены **Великобритания, Нидерланды и Австралия**

Несколько юридических тонкостей – 3

Выдержки из Федерального закона от 21 июля 2014 года N 242-ФЗ «О внесении изменений...», вступающего в силу с 1 сентября 2015 года

Дополнения в статью 18 ФЗ N 152

- (5) При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить *запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение* персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации
<http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=173429>

NB – в ФЗ N 242

- **Перечислены далеко не все действия в отношении ПДн**, определения которым даны в ФЗ N 152
- **Не приведено определение понятия «База данных** информации, содержащая персональные данные граждан РФ»

Несколько юридических тонкостей – 4

Выдержки из статьи 54 "Конституции Российской Федерации" (принята всенародным голосованием 12.12.1993) (с учетом нескольких поправок)

1. Закон, устанавливающий или отягчающий ответственность, обратной силы не имеет. http://www.consultant.ru/document/cons_doc_LAW_2875/?frame=1#p332

НВ – Конституция РФ обязывает операторов ПДн обеспечить их защиту в соответствии с текущими требованиями. Поэтому **по отношению к уже к находящимся в ЦОД Великобритании, Нидерландов и Австралии ПДн (т.е. ранее собранным)** и после 1 сентября 2015 г. можно без ограничений применять следующие действия: **использование, передачу (распространение, предоставление, доступ)** [в том числе – **трансграничную**], **обезличивание, блокирование, удаление, уничтожение**

Несколько юридических тонкостей – 5

В связи с отсутствием определения понятия «База данных информации, содержащая персональные данные граждан РФ», в качестве таковой можно использовать любую информационную систему, обеспечивающую запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн, например таблицу MS Excel *(и продолжать делать это до получения соответствующего замечания надзорного органа)*

Оператор должен обеспечить наполнение такой базы данных информацией;
желательна **автоматизация обеспечения целостности обновляемой информации**

Как минимизировать затраты операторов при переносе ПДн из ЦОД вне РФ

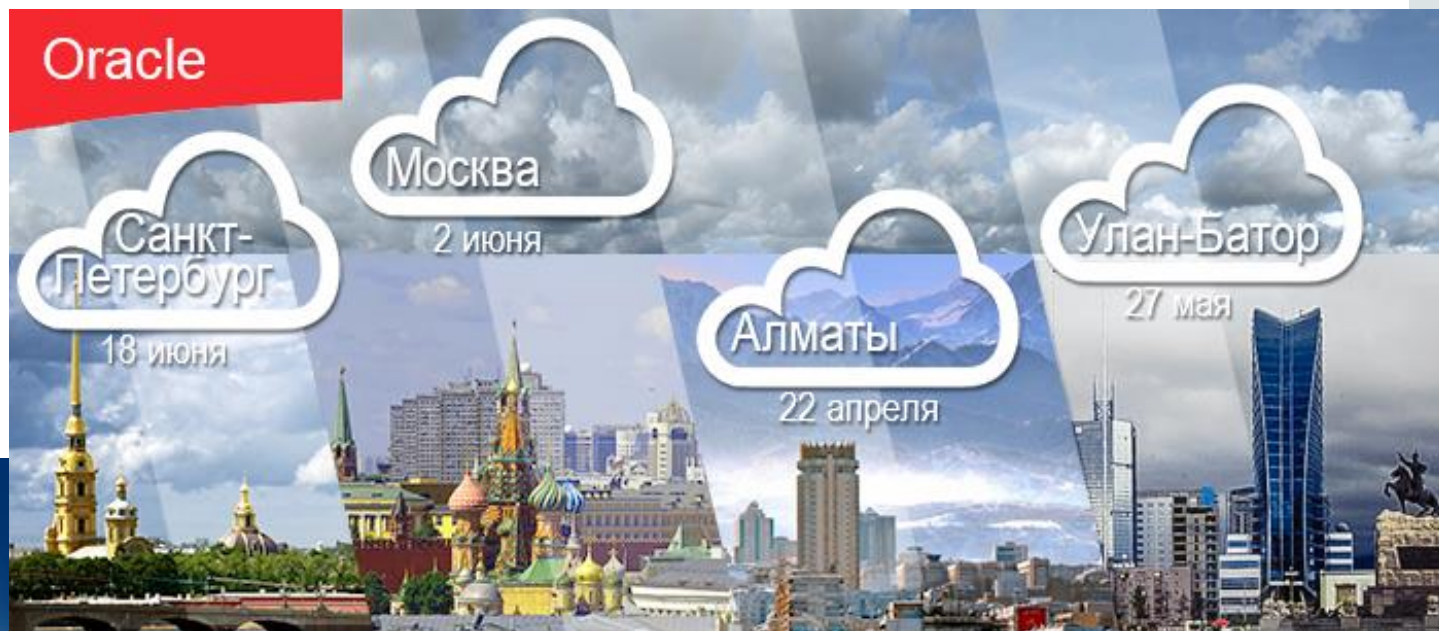
1. Завести и начать заполнять таблицу MS Excel новыми и обновляемыми ПДн; предусмотреть меры по ее защите
2. Внести соответствующие изменения в документы, определяющие политику оператора в отношении обработки ПДн
3. Оценить технологическую возможность и бюджет
 - а) полного переноса приложения с ПДн в ЦОД на территории РФ
 - б) переноса только ПДн в ЦОД на территории РФ
4. Предусмотреть правовые, организационные и технические меры по защите ПДн в ЦОД на территории РФ в соответствии со статьей 19 ФЗ N 152

Предложения Oracle по технологиям переноса и защиты ПДн в ЦОД на территории РФ

Наши локальные облачные партнеры для полного переноса приложений с ПДн в ЦОД на территории РФ



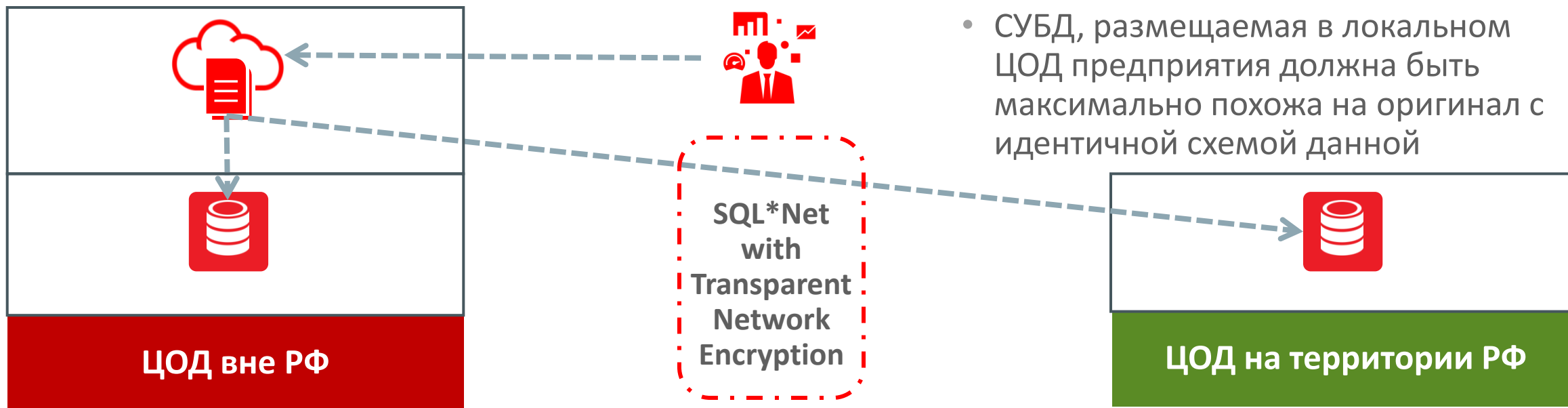
Hosting and Cloud Computing



<http://www.datafort.ru/press/novosti.html>

<http://www.fors.ru/en/solutions/cloud/>
<http://cloud.distr.fors.ru>

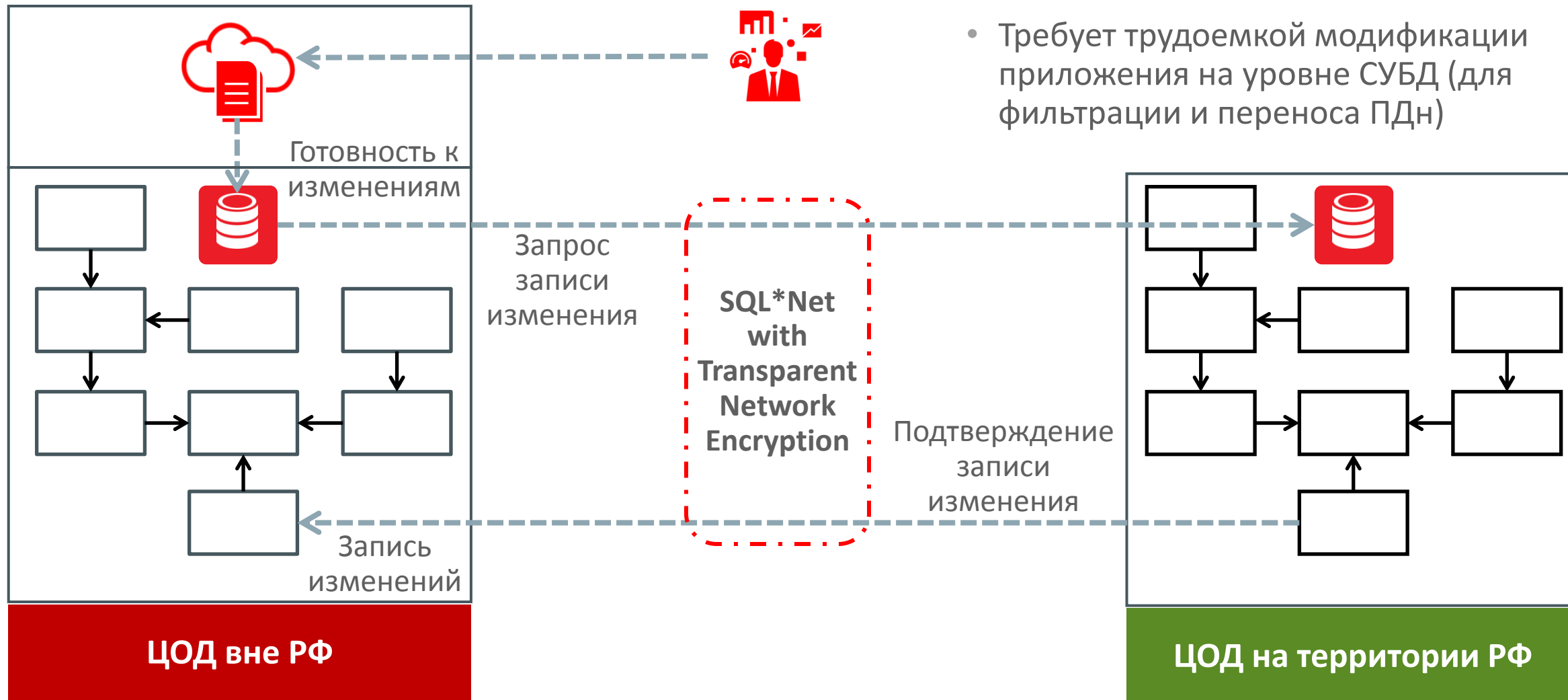
Распределенная (XA-) транзакция позволяет записать изменения сразу в два места



- Применимо для приложений, реализующих бизнес-логику на уровне Middleware (в AppServer)
- Требуе модификации на уровне Middleware функций вызова СУБД (для фильтрации и переноса ПДн)
- ПДн граждан РФ можно не дублировать в двух ЦОД, а физически разделить и перенести в Россию
- Требуе наличия инструмента для мониторинга и координации транзакций, например Oracle Tuxedo [wikipedia.org/wiki/Tuxedo \(software\)](http://wikipedia.org/wiki/Tuxedo_(software))

XA Транзакции - <http://dic.academic.ru/dic.nsf/ruwiki/1715630>

Двухфазная фиксация транзакции с помощью Oracle Database Link



Оптимальное решение – Oracle GoldenGate

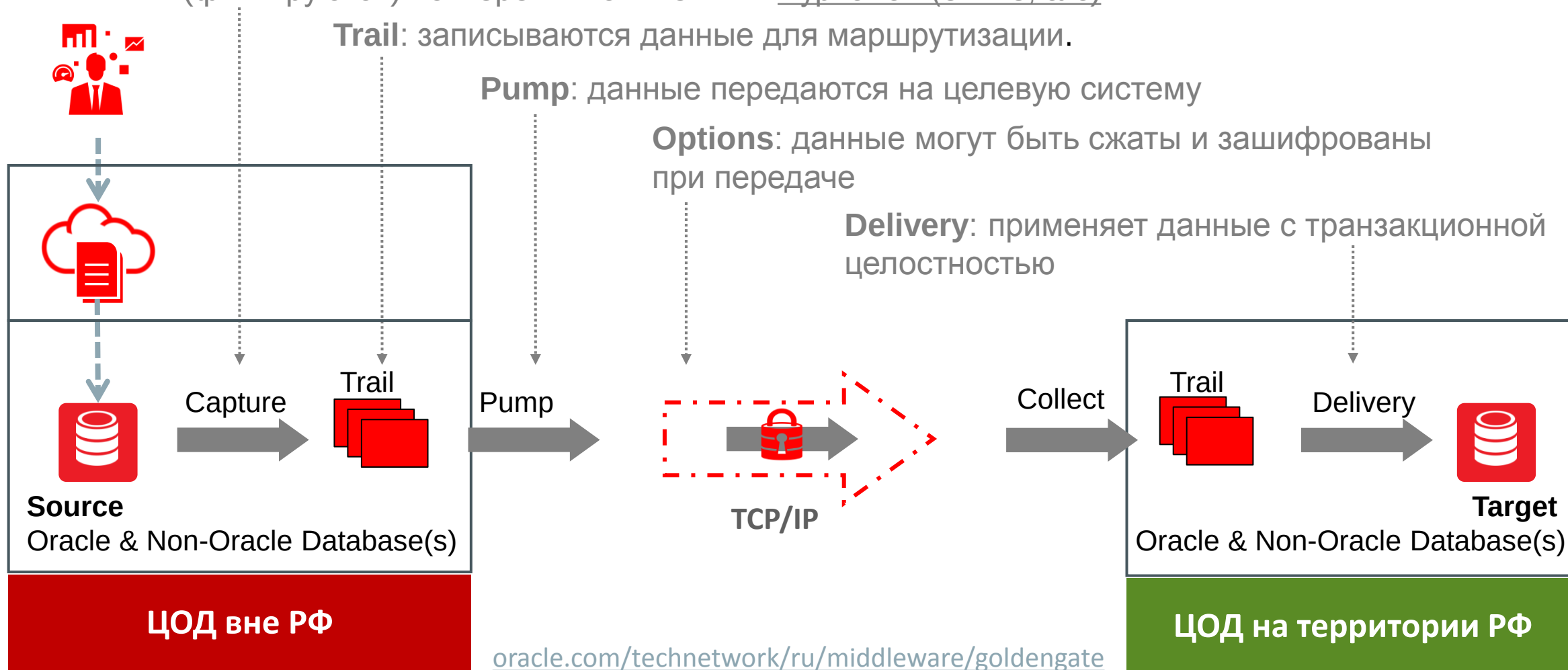
Capture: зафиксированные транзакции захватываются (фильтруются) по мере их появления в журналах (online, arc).

Trail: записываются данные для маршрутизации.

Pump: данные передаются на целевую систему

Options: данные могут быть сжаты и зашифрованы при передаче

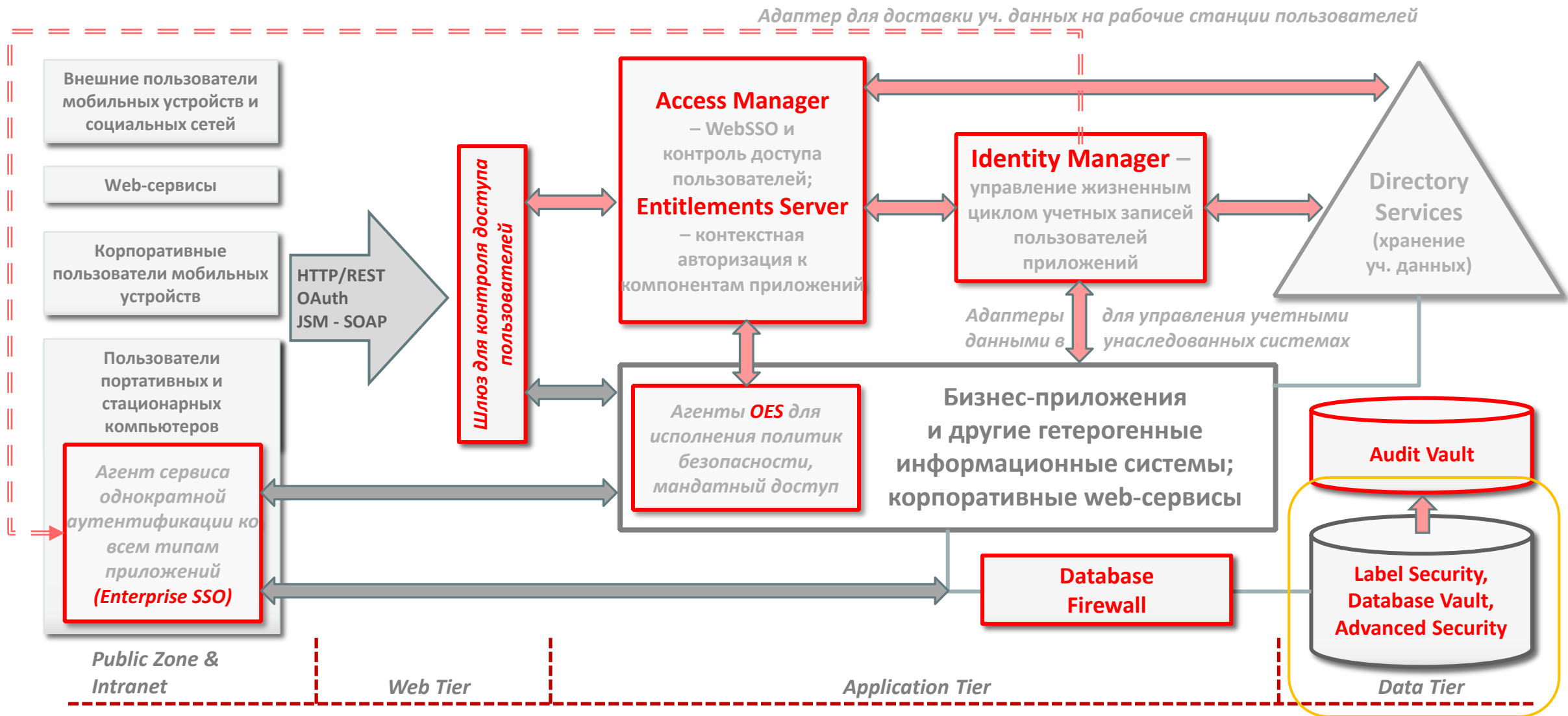
Delivery: применяет данные с транзакционной целостностью



Примеры выборки данных с помощью Oracle GoldenGate

- TABLE selection
 - MAP sales.tcustord, TARGET sales.tord;
- ROWS selection
 - WHERE (PRODUCT_TYPE = “AUTO”);
- OPERATIONS selection
 - FILTER (ON UPDATE, ON DELETE, amount > 0);
- COLUMNS selection (COLS и COLSEXCEPT)
 - TABLE sales.tcustord, TARGET sales.tord, COLSEXCEPT (facility_number);

Соответствие требованиям через экстернализацию средств защиты приложений в сертифицированные решения Oracle



Средства безопасности, сертифицированные ФСТЭК



Максимальная
производительность
на базе инженерных
систем Oracle

#3215 – Oracle Database
на Exadata – механизмы
защиты СУБД

#3299 – Oracle Fusion Middleware
на Exalogic – механизмы защиты Java
(FMW Platform Security Services)

Максимальный
уровень
защищенности
(СВТ НСДЗ+НДВ2)

#3095 – Oracle
Enterprise Linux (OEL)
– механизмы защиты
операционной
системы

#3196 – Oracle Fusion
Middleware на серт. OEL
– механизмы защиты
Java (FMW Platform
Security Services)

#3295 – Oracle Identity & Access
Management на серт. OEL –
механизмы защиты сервисов
безопасности (Identity Manager,
Access Manager & Entitlements Server)

Защита
гетерогенных
сред

#2858 – Oracle
Database на OEL,
Solaris & Windows –
механизмы защиты
СУБД (высокий
уровень защиты
при использовании
серт. OEL)

#3364 – Oracle
Audit Vault &
Database Firewall
– межсетевой
экран для SQL-
трафика и защита
данных аудита

#3103 – Oracle
Enterprise Single
Sign-On для среды
Windows –
идентификация и
аутентификация,
регистрация событий
безопасности

#2238 – Oracle Identity
& Access Management
– механизмы защиты
сервисов
безопасности (Identity
Manager & Access
Manager)

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



andrey.gusakov@oracle.com

+7495-6411400

security-orcl.blogspot.ru

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** (срок действия истек)
- 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); **имеется 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; **имеется 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

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**
- 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**

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); **имеется серт. ФСТЭК**
- 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

Внедрение средств защиты приложений в ЦОД

Mobile Security

- Без ущерба для комфорта владельца мобильного устройства обеспечивает изоляцию (контейнеризацию) корпоративных данных и приложений, их шифрование и применение политик безопасности, направленных на борьбу с утечками
- Реализует SSL-туннель уровня приложения между корпоративной системой контроля доступа и контейнером, что исключает необходимость организации VPN на уровне мобильного устройства и защищает от вредоносных приложений
- Предоставляет несколько готовых к использованию защищенных мобильных приложений, средства их распространения и набор инструментов для встраивания функций безопасности как в собственные приложения, так и в решения сторонних разработчиков
- Прединтегрирован со средами Microsoft Active Directory, Oracle Identity & Access Management; поддерживает платформы iOS и Android, в ближайших планах – Windows Phone; запланирована сертификация во ФСТЭК