

ORACLE®

# Обзор средств защиты OracleAS 10G

**Игорь Лукьянов**

Старший консультант  
Oracle Application Server 10g

# Что такое Identity Management?

*“Identity management – это процесс, с помощью которого обеспечивается полный цикл защиты пользователей и других связанных объектов в системе за счет операций управления и контроля для организации или группы организаций.”*

# Identity Management Инфраструктура

- Корпоративная служба каталогов - Oracle Internet Directory (OID)
  - Каталог пользователей, групп, приложений, ролей & установленных правил
- Службы управления доступом
  - Single Sign-on (SSO)
  - Централизованный репозиторий авторизации (в OID)
- Платформа обеспечения IM - Directory Integration and Provisioning (DIP)
  - Реализация установленных правил и утилиты управления учетными записями (accounts)
  - Интеграционная платформа обеспечения IM
    - Обеспечение распространения событий, автоматизация последовательности событий
    - Коннекторы обеспечения IM
    - Платформа мета-каталогов и коннекторов
      - Служба Directory Synchronization (DSS)

# Identity Management Инфраструктура

- **Delegated Administration Services (DAS)**
  - Утилиты самообслуживания конечных пользователей
  - Утилиты управления корпоративными пользователями, группами и ролями
  - Административные утилиты делегирования полномочий для приложений
- **Public Key Infrastructure (PKI) службы**
  - Oracle Certificate Authority (OCA)
  - Certificate / key архивы
  - Интерактивная проверка статуса сертификатов
- **Службы мониторинга аудита и защиты**
  - Утилиты управления корпоративными правилами аудита
  - Централизованный архив лог-файлов аудита и утилиты для обеспечения аудита

# Проблема растущей пользовательской среды

- Растущее число корпоративных приложений
  - Новые Web-приложения и унаследованные системы (Legacy Systems)
  - Интеграция новых приложений с унаследованными системами
- Растущая популяция пользователей
  - Возможность самообслуживания пользователей для доступа к корпоративным приложениям
- Виртуальный доступ пользователей
  - Обеспечение доступа с любого устройства, откуда-либо, и из любой сети
- Появление новых бизнес-моделей
  - Защищенное расширение бизнес-процессов в корпоративной сети
- Новые нормативные требования
  - Гарантирование согласованности с корпоративными и правительственными правилами секретности

# Потребительские проблемы

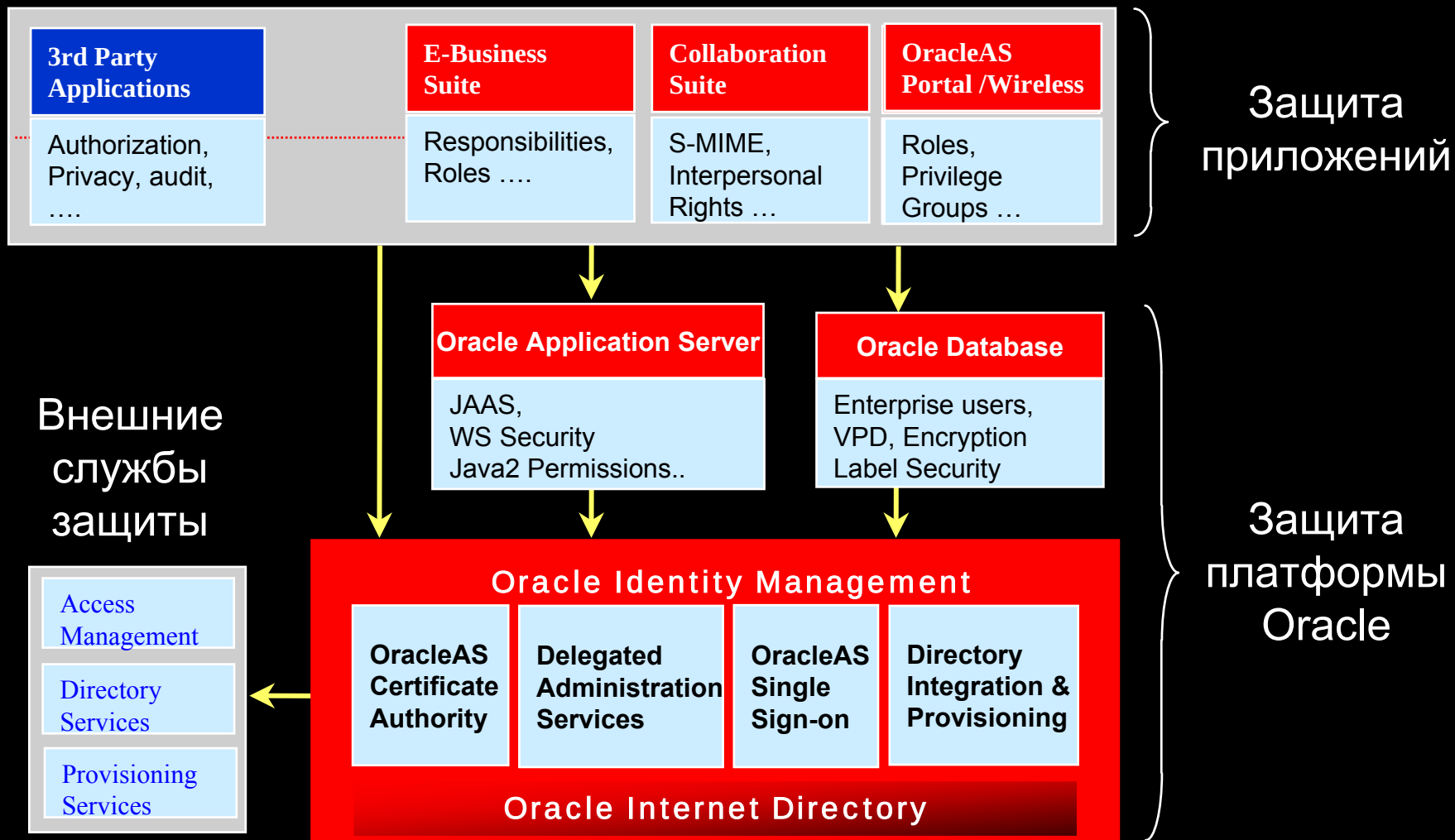
- Растущие административные проблемы
  - Комплексность задачи обеспечения защищенности пользователей (объяснить)
  - Ограниченная возможность делегировать администрацию
  - Рост цены обслуживания с появлением новых пользователей, приложений и устройств
- Фундаментальные проблемы администрирования
  - Много пользовательских учетных записей, привилегий и паролей
  - Трудности получения доступа к введенным в эксплуатацию системам
  - Неадекватная персонализация информации
- Рост уязвимости защиты информации
  - Корпоративная защита является фрагментированной
  - Ограниченная видимость потенциальных уязвимостей
  - Невозможность определять непротиворечивые правила регулирования доступа

# Потребительская выгода использования Oracle Identity Management

- **Сохранение денег**
  - Централизованное управление учетными записями снижает стоимость администрирования
  - Упрощение автоматизации и уменьшение ошибок
- **Улучшение защиты**
  - Уменьшение фрагментированности защиты
- **Расширение удобств для пользователя**
  - Простой пароль и Single Sign-on
  - Персонализация
  - Делегированная администрация и самообслуживание



# Общая архитектура защиты Oracle



# Компоненты Oracle Identity Management архитектуры

# Требования к Oracle Identity Management Архитектуре

- Корпоративная интеграция
- Высокая готовность
- Масштабируемость
- Секьюрити
- Интеграция с продуктовой линией Oracle
- Поддержка стандартов

# Компоненты Oracle Identity Management Архитектуры

**Oracle Internet Directory**

**Directory Integration & Provisioning**

**Delegated Administration**

**Single Sign-On**

**Certificate Authority**

# Oracle Internet Directory

- Масштабируемость
  - Миллионы пользователей
  - Тысячи одновременно работающих клиентов
- Высокая готовность
  - Репликация
  - Hot backup/recovery, RAC, и т.д.
- Управляемость
  - Мониторирование многих серверов
- Защита
  - Сложное паролирование
  - Контроль доступа
  - Аудит
- Расширяемость (Plug-in framework)
  - Виртуальные атрибуты
  - Внешняя аутентификация
  - Заказные правила для паролирования

LDAP  
Клиенты



Directory  
Admin  
Console

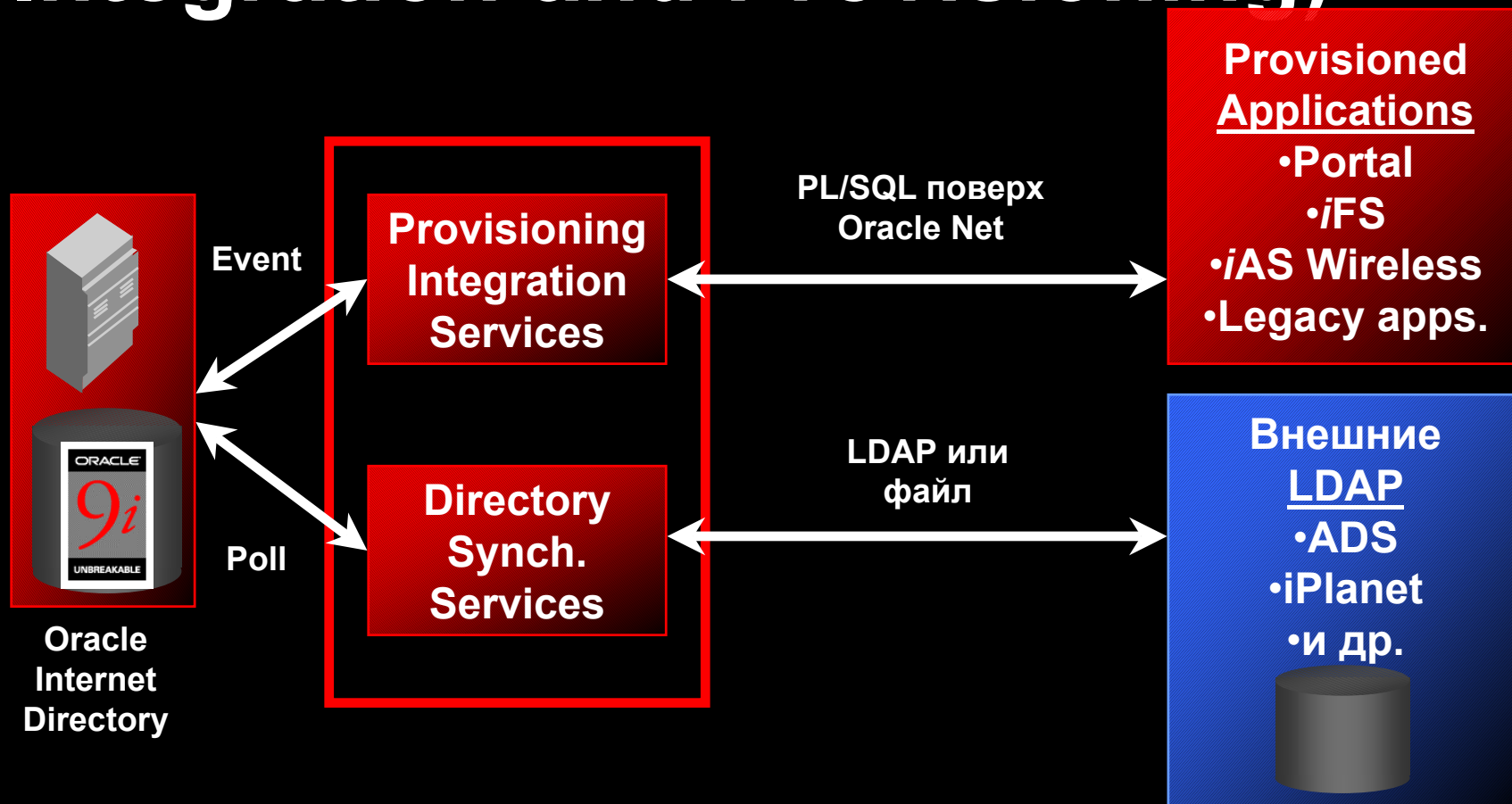


Oracle  
Internet  
Directory  
Server



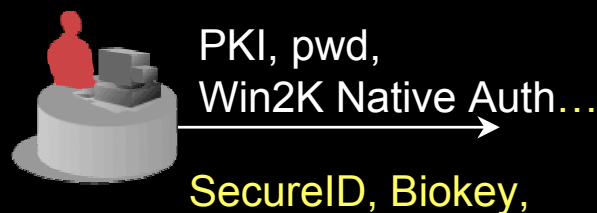
Oracle  
RDBMS

# Служба DIP (Directory Integration and Provisioning)

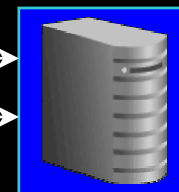


# OracleAS Single Sign-On

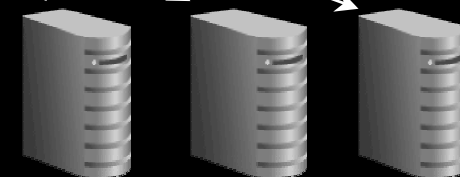
- Использование single sign-on для всех Oracle web-based приложений



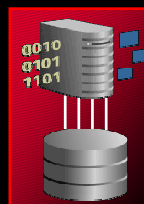
OracleAS Возможное окружение



Partner SSO (Netegrity, RSA, Oblix)



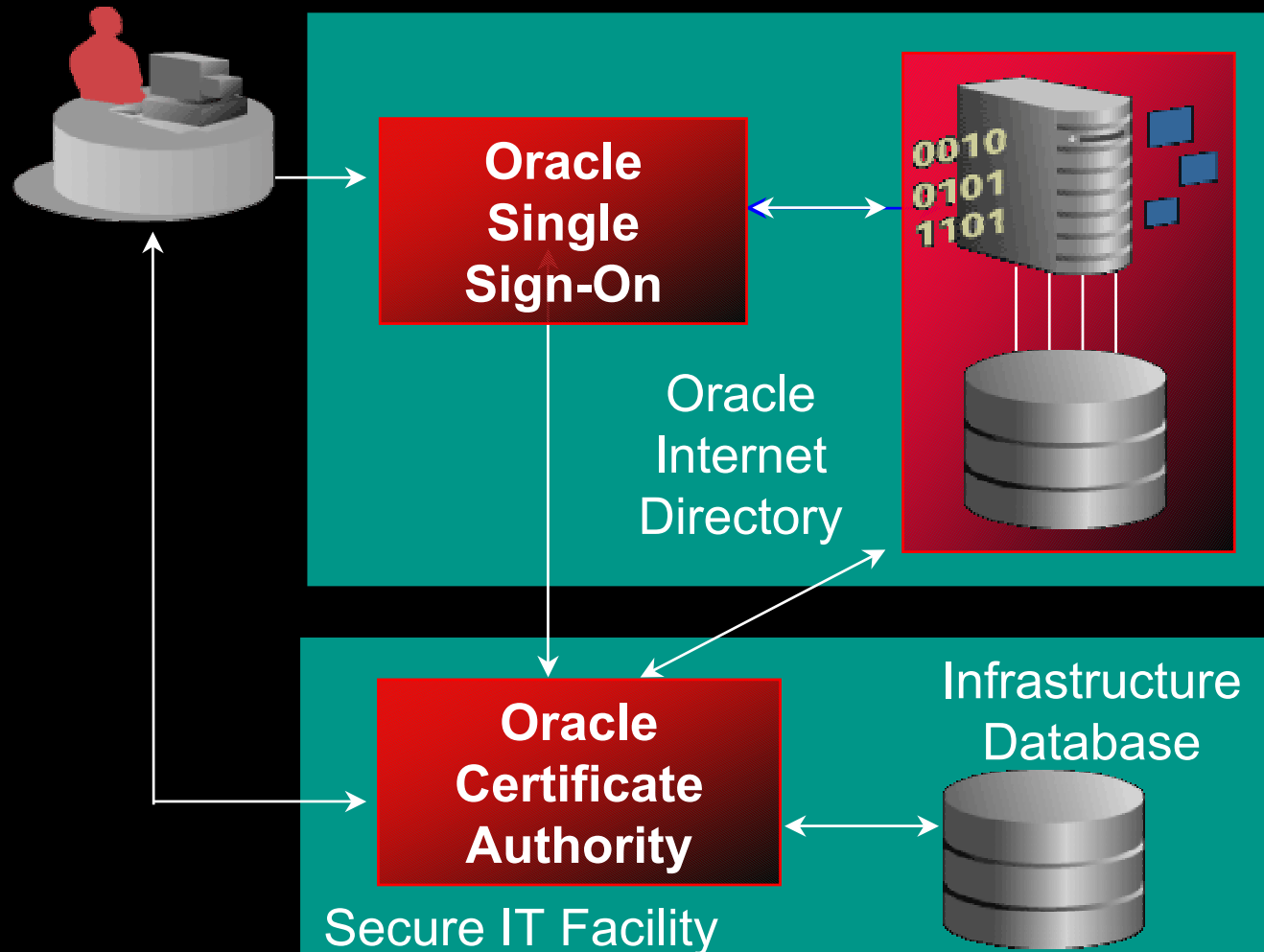
Партнерское SSO  
Возможное окружение



OID

ORACLE®

# OracleAS Certificate Authority





# Delegated Administration Services

Administration.Create User.Information - Microsoft Internet Explorer

File Edit View Favorites Tools »

Address [oiddas/ui/oracle/ldap/das/admin/DASCreateUserInfoAdmin?clearcache=true](#)

**ORACLE**  
Internet Directory

Home My Profile **Directory** Configuration

Users Groups

▼ Password Management ▼ Additional Information ▼ Work Address ▼ Home Address ▼ Contact Numbers ▼ Photo Management ▼ Resource Assignment

Cancel Submit

### Create User

#### Basic Information

Create

\* User ID

\* First Name

\* Last Name

\* Title

\* Employee Number  (numbers only)

\* indicates a Required Field.

#### Password Management

[Return to Top](#)

\* Password

\* Confirm Password

\* indicates a Required Field.

#### Additional Information

[Return to Top](#)

Done Local intranet

# Окружение работающих приложений для Oracle AS

# Окружение работающих приложений для Oracle AS



- Mail
- Voicemail
- Calendar
- Files
- iMeeting
- etc.



- Supply chain mgmt
- Marketing & sales mgmt
- Service mgmt
- Financial mgmt
- Project mgmt
- HR mgmt
- Vertical applications ...

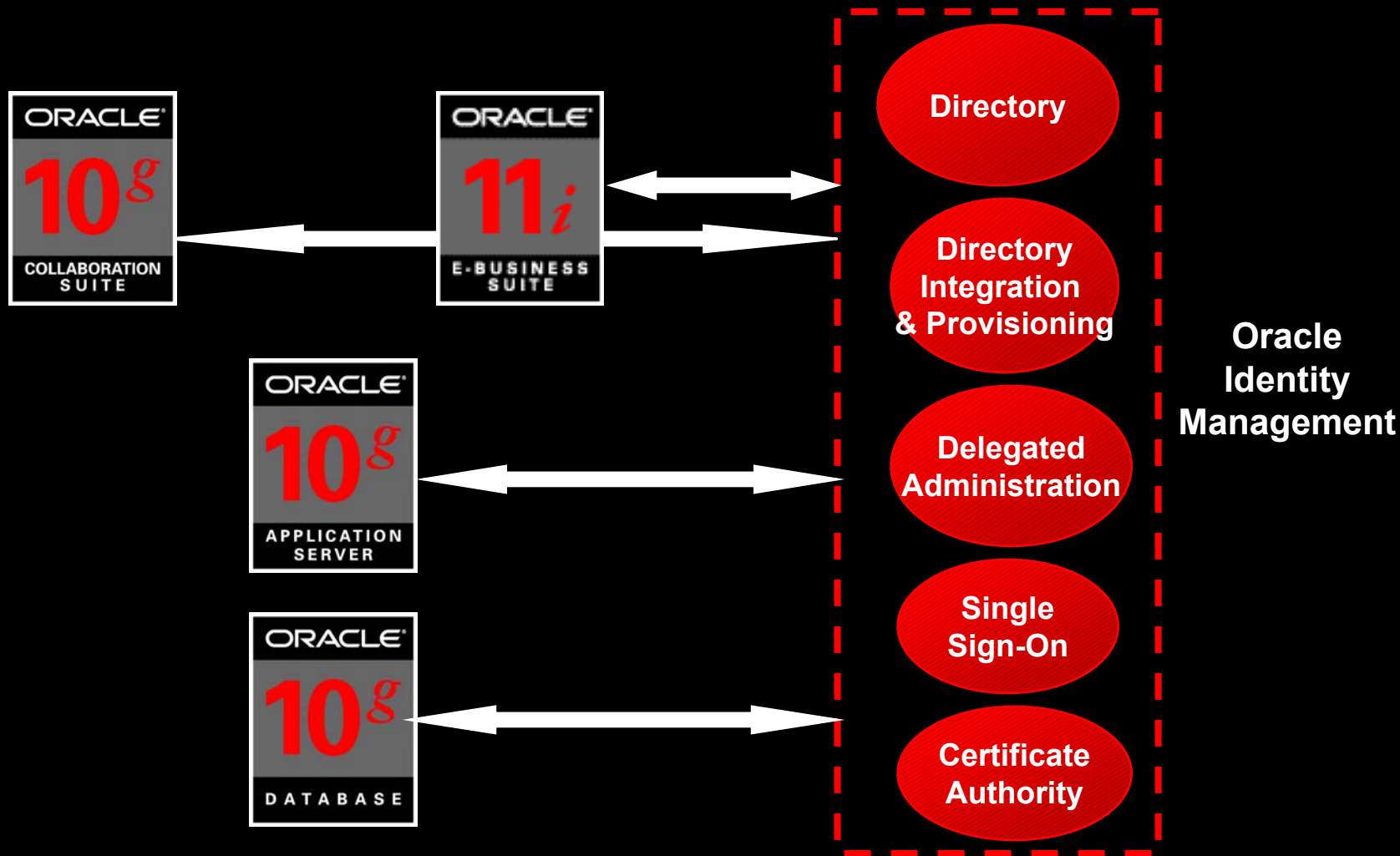


- HTTP server
- Web services
- Portal
- Web cache
- Forms
- Reports
- etc.

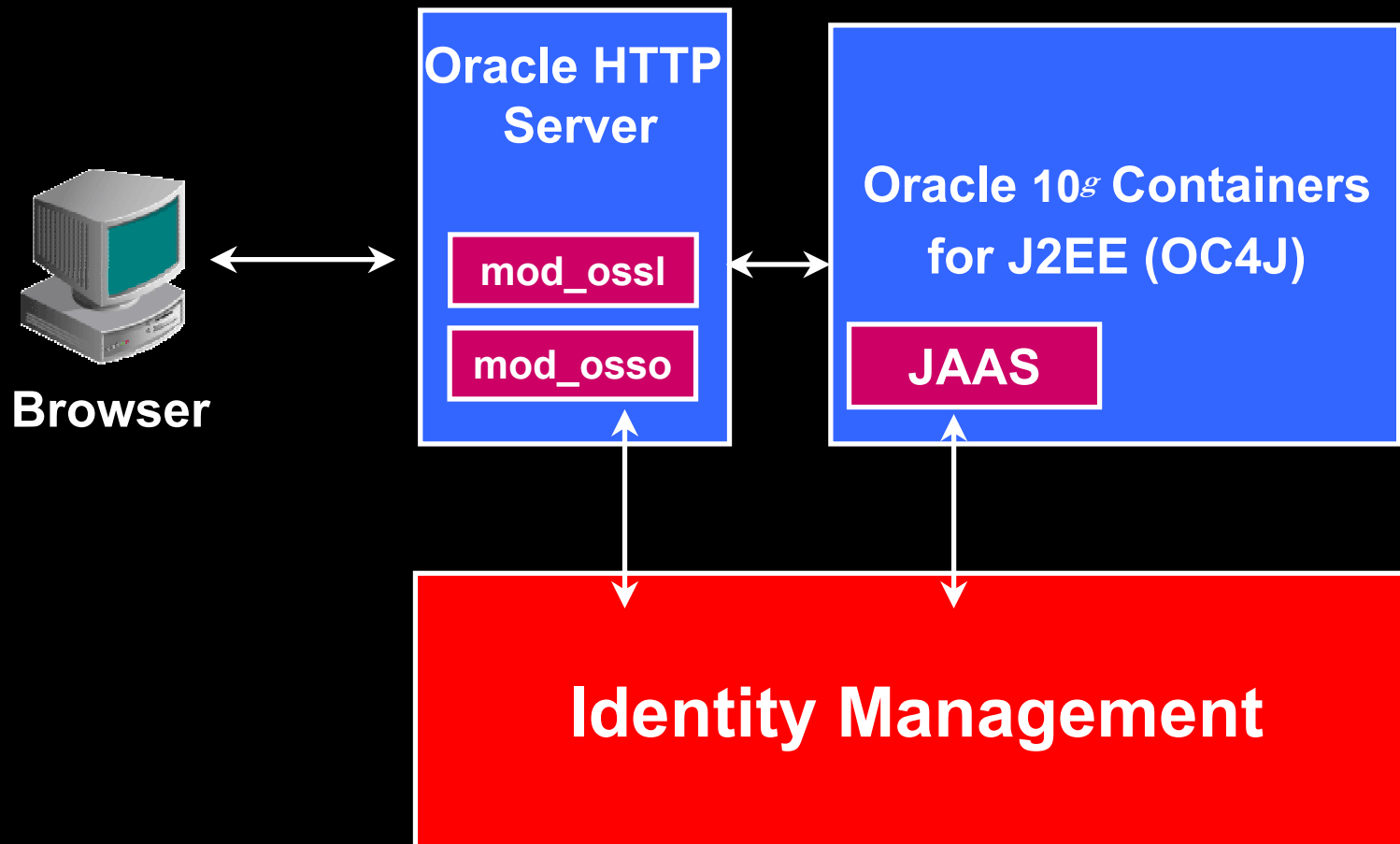


- Oracle Database
- Oracle Label Security

# Окружение работающих приложений для Oracle AS

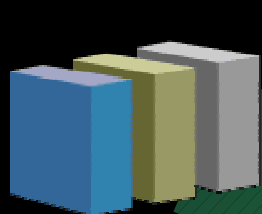


# Защита Oracle Application Server с Identity Management

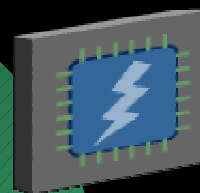


# Enterprise Grid Computing с Identity Management.

Виртуализация  
и пул ресурсов



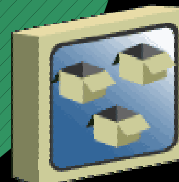
Высокое  
качество  
обслуживания



Обслуживание  
приложений на  
различных  
уровнях



Автоматизация  
Обслуживания  
Пользователей и  
ресурсов



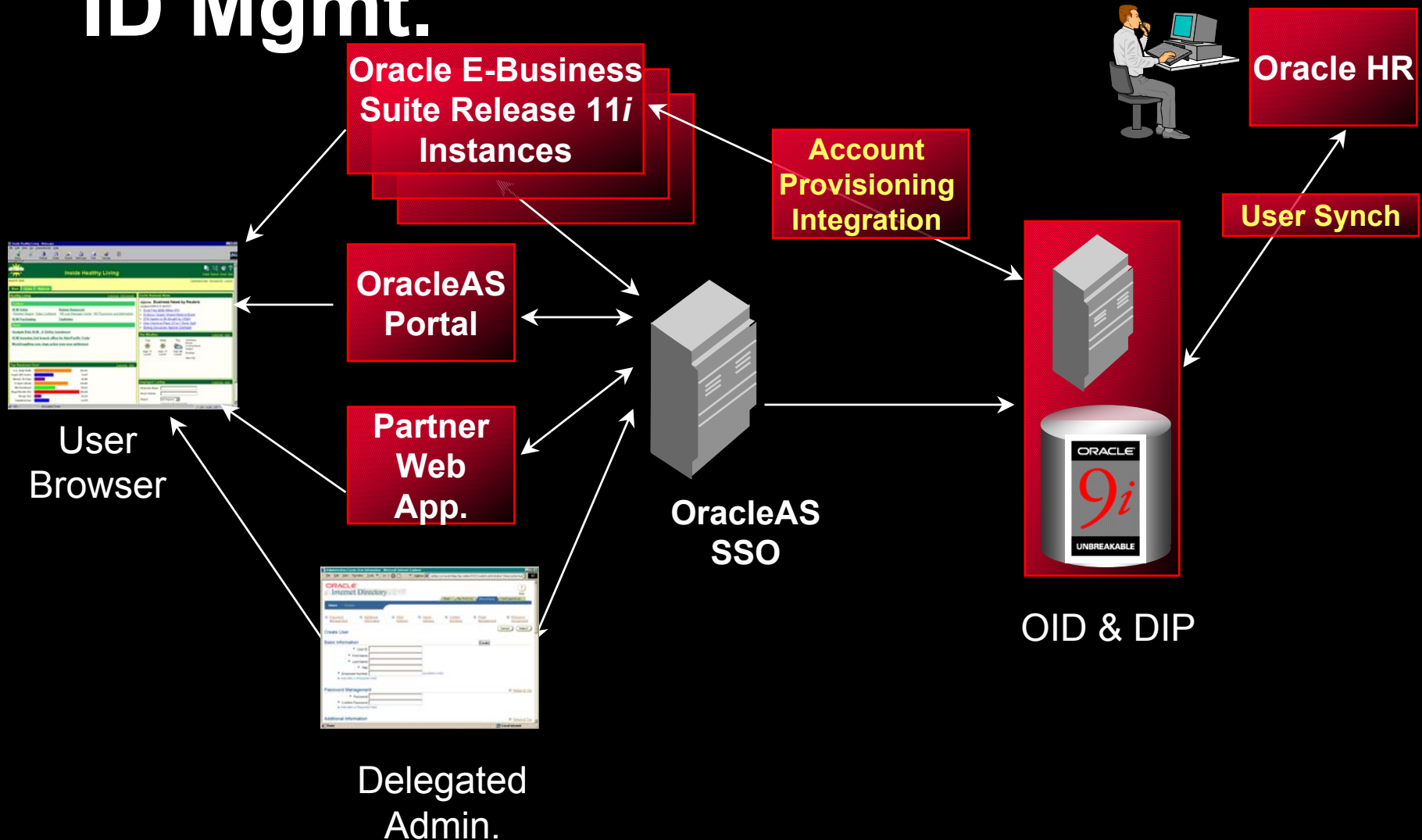
10g

# Защита Oracle Database с Identity Management



**Корпоративная защита пользователей**

# Oracle E-Business c ID Mgmt.



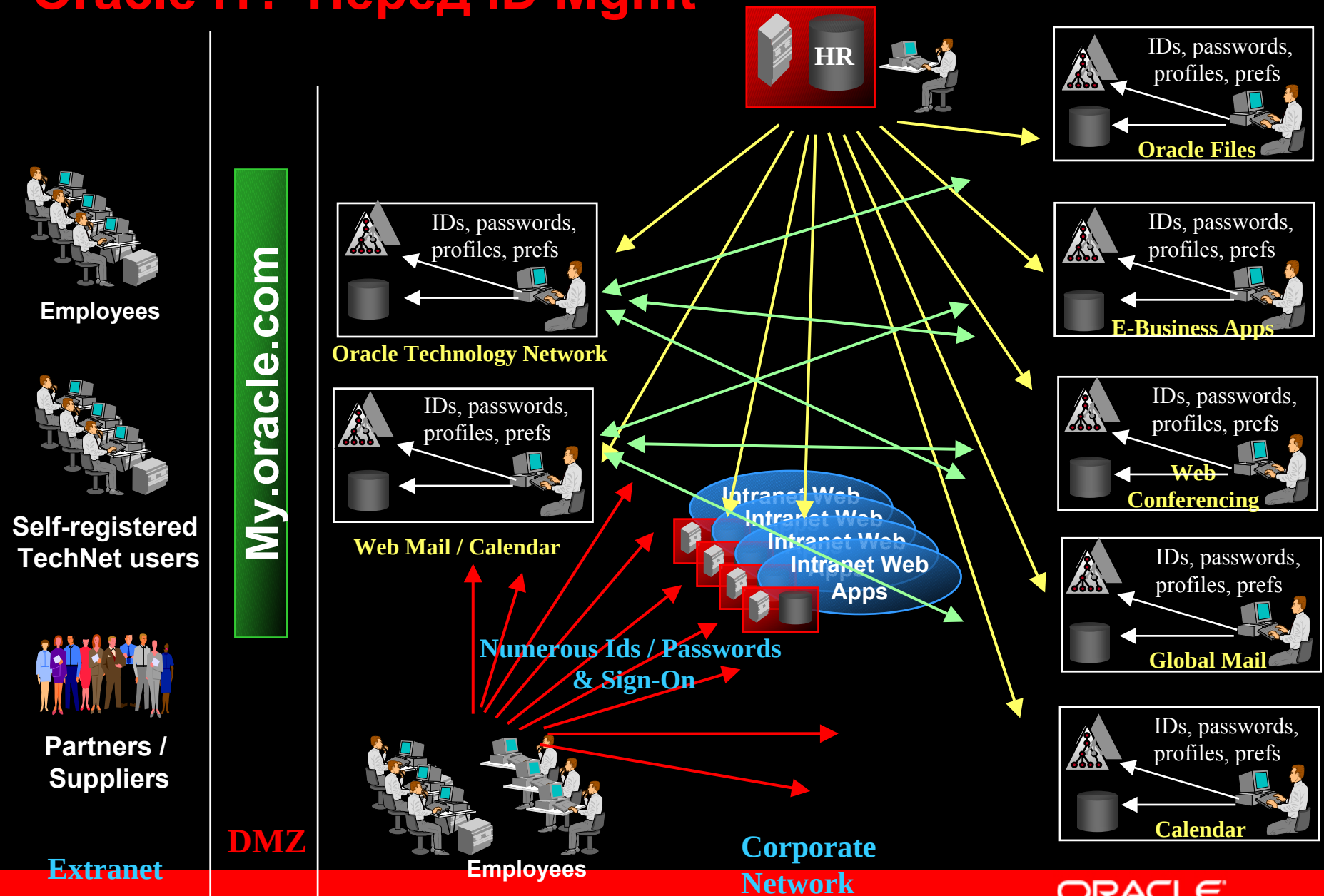


# **Использование Identity Management Архитектуры на примере самой компании Oracle Corporation**

# Oracle Global IT

- Проблема
  - Множество приложений с ID/password
  - 40,000 работников и 3.5Миллиона Oracle Technology Network пользователей
  - Множество порталов для сотрудников и несотрудников
  - Множество одновременно разрабатываемых приложений с разными отчетными периодами
- Решение
  - Использование Identity Management Архитектуры

# Oracle IT: Перед ID Mgmt



# Oracle IT: После ID Mgmt



Employees



Self-registered  
TechNet users

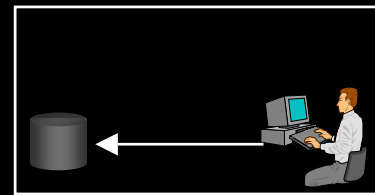


Partners /  
Suppliers

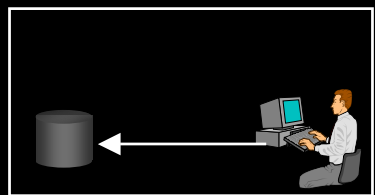
Extranet

My.oracle.com

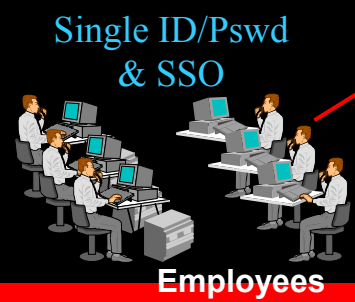
DMZ



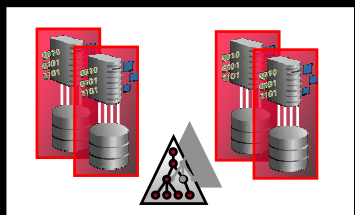
Oracle Technology Network



Web Mail / Calendar



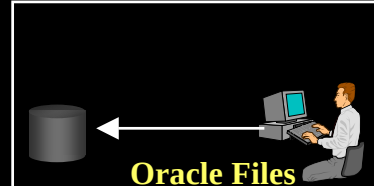
Employees



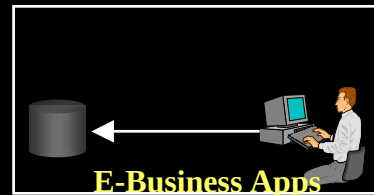
Oracle IdM  
Infrastructure



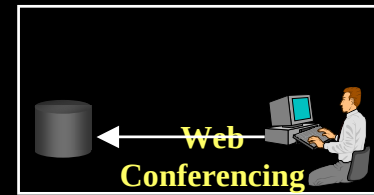
Corporate  
Network



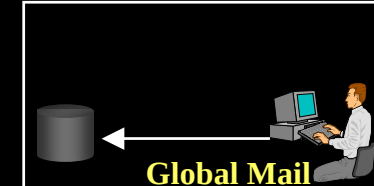
Oracle Files



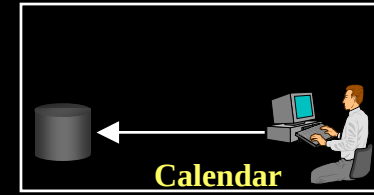
E-Business Apps



Web  
Conferencing



Global Mail



Calendar

ORACLE

# Где найти больше информации

- Oracle WWW-сервер
  - <http://oracle.com/security/>
- Oracle Technology Network
  - [http://otn.oracle.com/products/id\\_mgmt/](http://otn.oracle.com/products/id_mgmt/)
- Oracle University
  - <http://education.oracle.com/> -> Enterprise Identity Management

A large, stylized graphic in the background consisting of a grey 'Q' and 'A' with a red ampersand in the center. The text 'Вопросы' and 'Ответы' is overlaid on the ampersand.

# Вопросы Ответы

ORACLE®