RISSPA

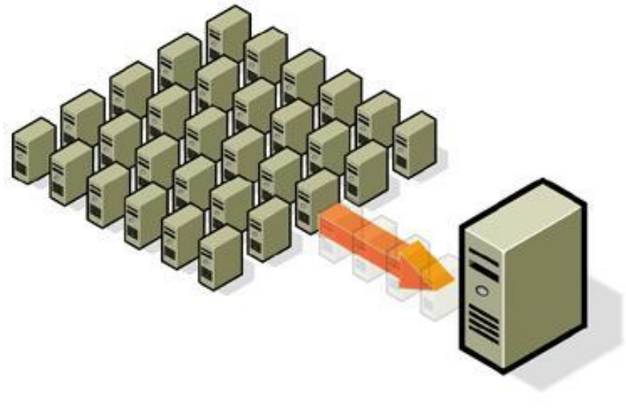
Современные риски информационной безопасности и подходы к их минимизации

Конференция «Управление инвестициями и инновациями в информационных технологиях»
02 марта 2012 г.

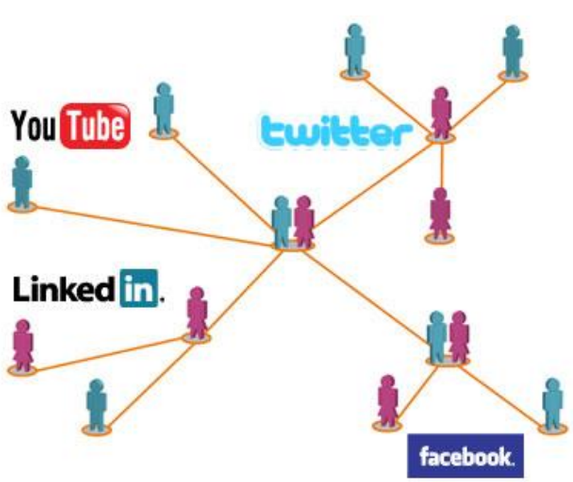
Евгений Климов,
CISM, CISSP, CCSK, PMP

Президент RISSPA

Современные вызовы



Облачные сервисы и технологии виртуализации



Социальные сети

Мошеннические операции

Мобильные устройства

Облачные вычисления и виртуализация

RISSPA
be professional

Сервисная модель

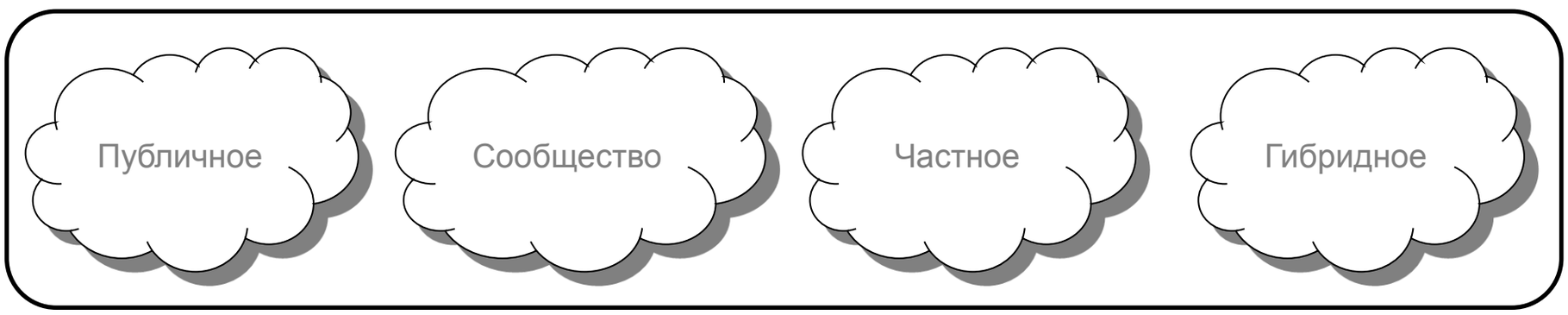
IaaS Инфраструктура как сервис	PaaS Платформа как сервис	SaaS Приложение как сервис	xaaS

Ключевые характеристики

Сетевой доступ	Эластичность	Измеримый сервис	Сервис по запросу

Разделение ресурсов

Модель развертывания



Облачные вычисления и виртуализация

RISSPA
be professional

Основные преимущества:

- Снижение капитальных расходов (публичное облако)
- Прозрачность ценообразования
- Оплата только используемых ресурсов
- Эффективное использование ресурсов
- Эластичность и неограниченность ресурсов
- Быстрота развертывания
- Выход на новые рынки
- Обеспечение потребностей бизнеса

Облачные вычисления и виртуализация

RISSPA
be professional

Риски безопасности:

•Доверие: прозрачность сервис-провайдера, процедуры контроля и управления рисками, соответствие законодательству

•Безопасность данных: утечка, доступность, потеря, место размещения данных

•Уязвимости в программном обеспечении

•Отсутствие стандартизации

•Совместное использование ресурсов

•Атаки на учетные записи

•Инсайдеры

•Необходимость специализированных средств защиты

Облачные вычисления и виртуализация

RISSPA
be professional

Апрель 2011

Dropbox

«Как у большинства онлайн-сервисов у нас есть ограниченный перечень сотрудников, которым разрешен доступ к пользовательским данным по причинам, указанным в нашей политике безопасности.»

«Системный администратор удалил виртуальные сервера бывшего работодателя. Оцениваемый размер ущерба составил 300 000%»

http://www.justice.gov/usao/nj/Press/files/Cornish,%20Jason%20News%20Release.html

Облачные вычисления и виртуализация

RISSPA
be professional

DigiNotar®
A VASCO COMPANY

Июль 2011

https://
Google

PlayStation®
Network

Апрель 2011

Март 2011

Облачные вычисления и виртуализация

RISSPA
be professional

Механизмы защиты:

•Актуализация стратегии безопасности, политик и процедур оценки и управления рисками с учетом специфики используемых сервисов

•Процедура оценки защищенности сервис-провайдеров

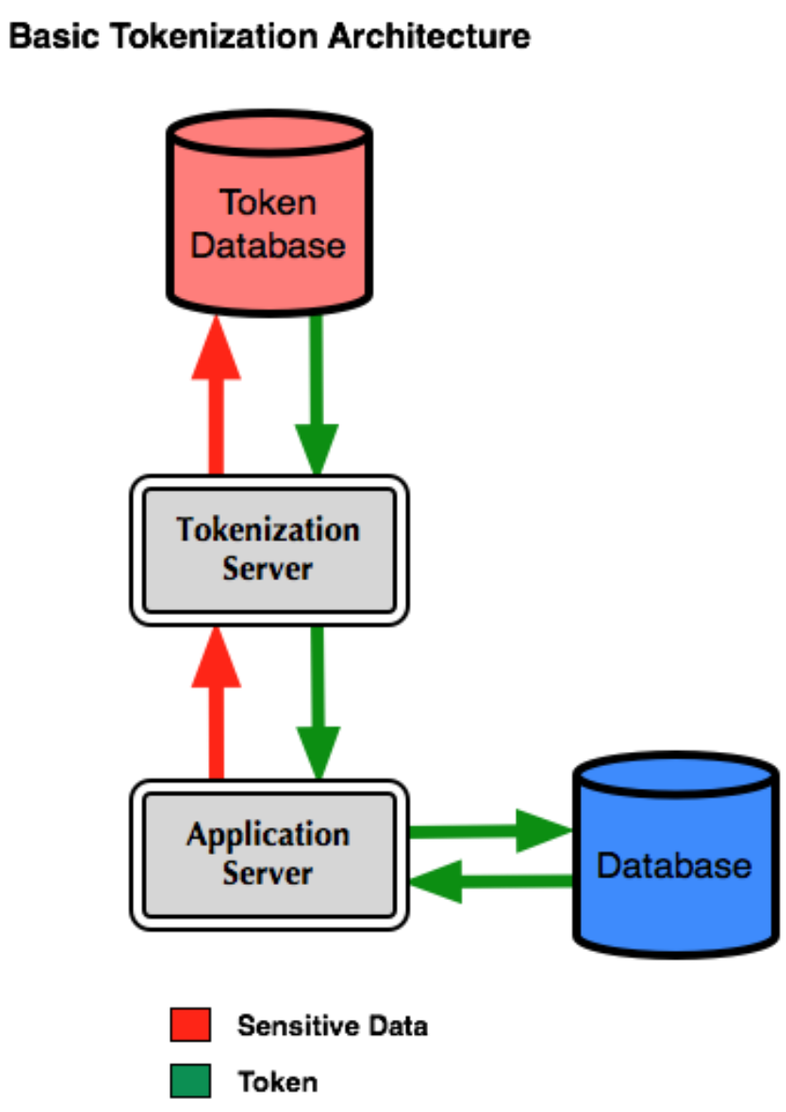
•Политики и процедуры защиты мобильных устройств

•Актуализация стратегии непрерывности бизнеса

•Использование специализированных средств защиты (контроль доступа, контроль утечек, мониторинг событий, криптографическая защита, токенизация, удаленное управление мобильными устройствами и др.)

•Повышение квалификации персонала подразделений информационной безопасности и внутреннего аудита

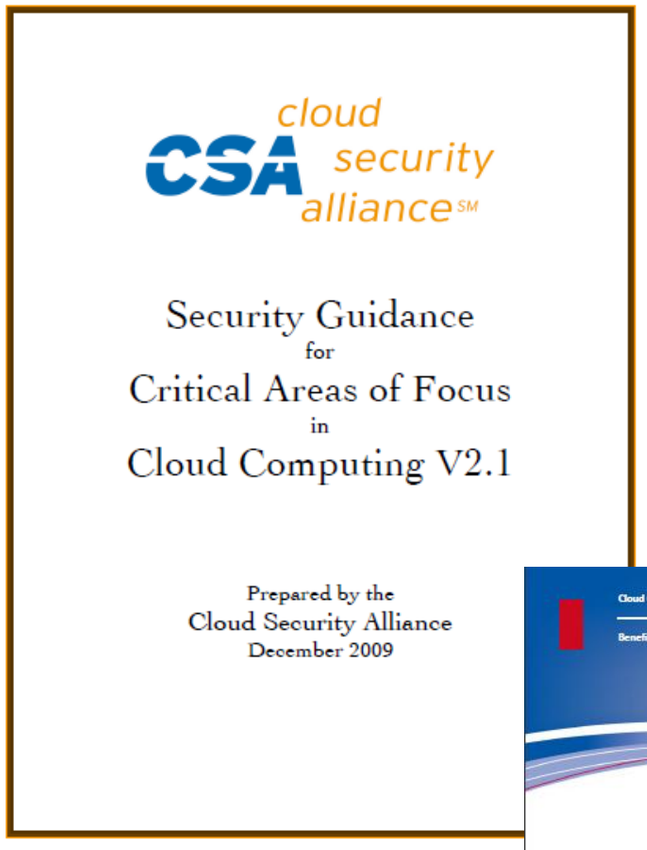
•Повышение осведомленности пользователей

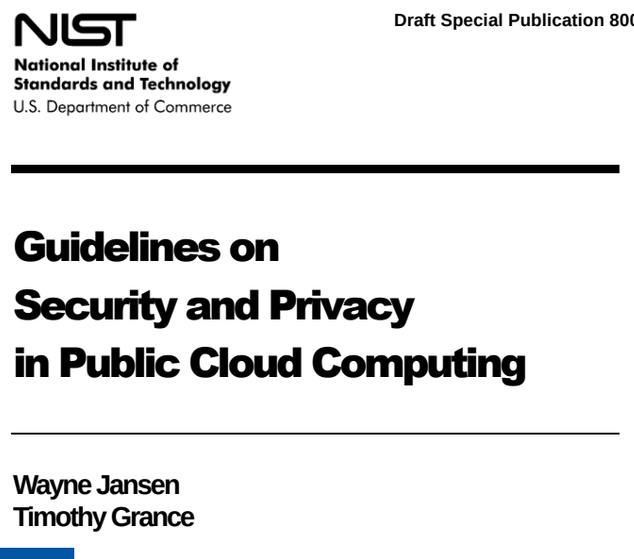


Токенизация

Облачные вычисления и виртуализация

RISSPA
be professional





Социальные сети

RISSPA
be professional

Риски:

•Неконтролируемое распространение информации

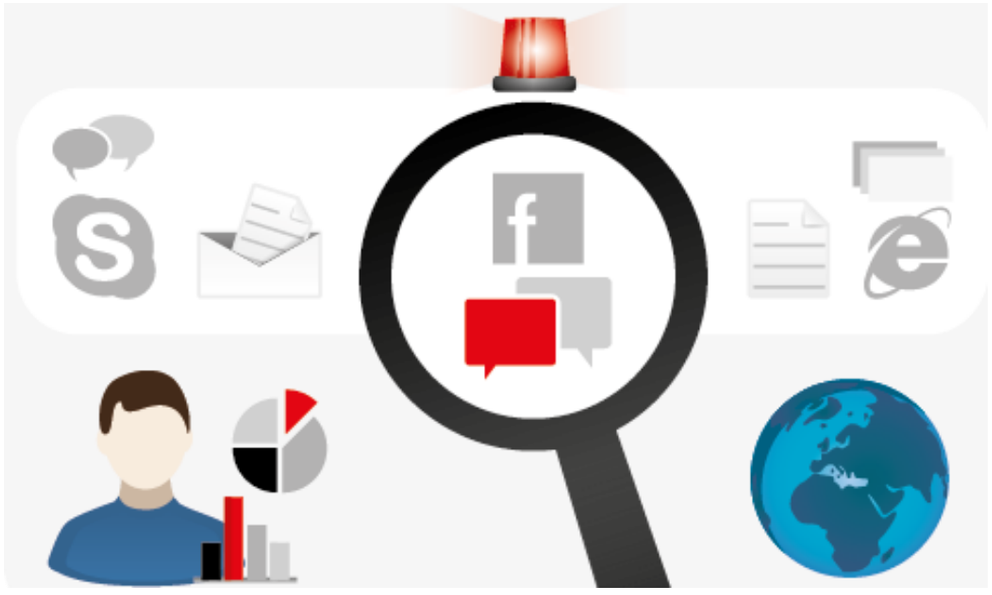
•Анонимность

•Невозможность удаления «цифровой» личности

•Кража личности/мошенничества

Социальные сети

RISSPA
be professional



Системы мониторинга

Политики и инструкции

Мошеннические операции

RISSPA
be professional

Уровень бизнес-процессов

- Интеграция в систему управления бизнес-рисками
- Выявление и предотвращение мошенничеств (фрод)
- Безопасность бизнес-приложений

Мониторинг инцидентов	Антивирусная защита	Межсетевые экраны	Контроль утечек
Управление доступом	Криптографическая защита		Обнаружение атак

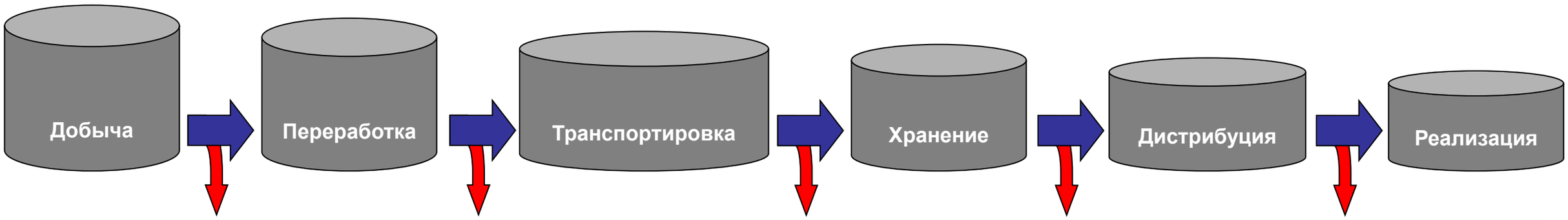
Уровень инфраструктуры

Мошеннические операции

Сектор	Средние потери, % от общей выручки
Финансовые организации	1-2%
Здравоохранение	5-10%
Телекоммуникации	2-5%+
Производство	2-5%

Исследование PWC

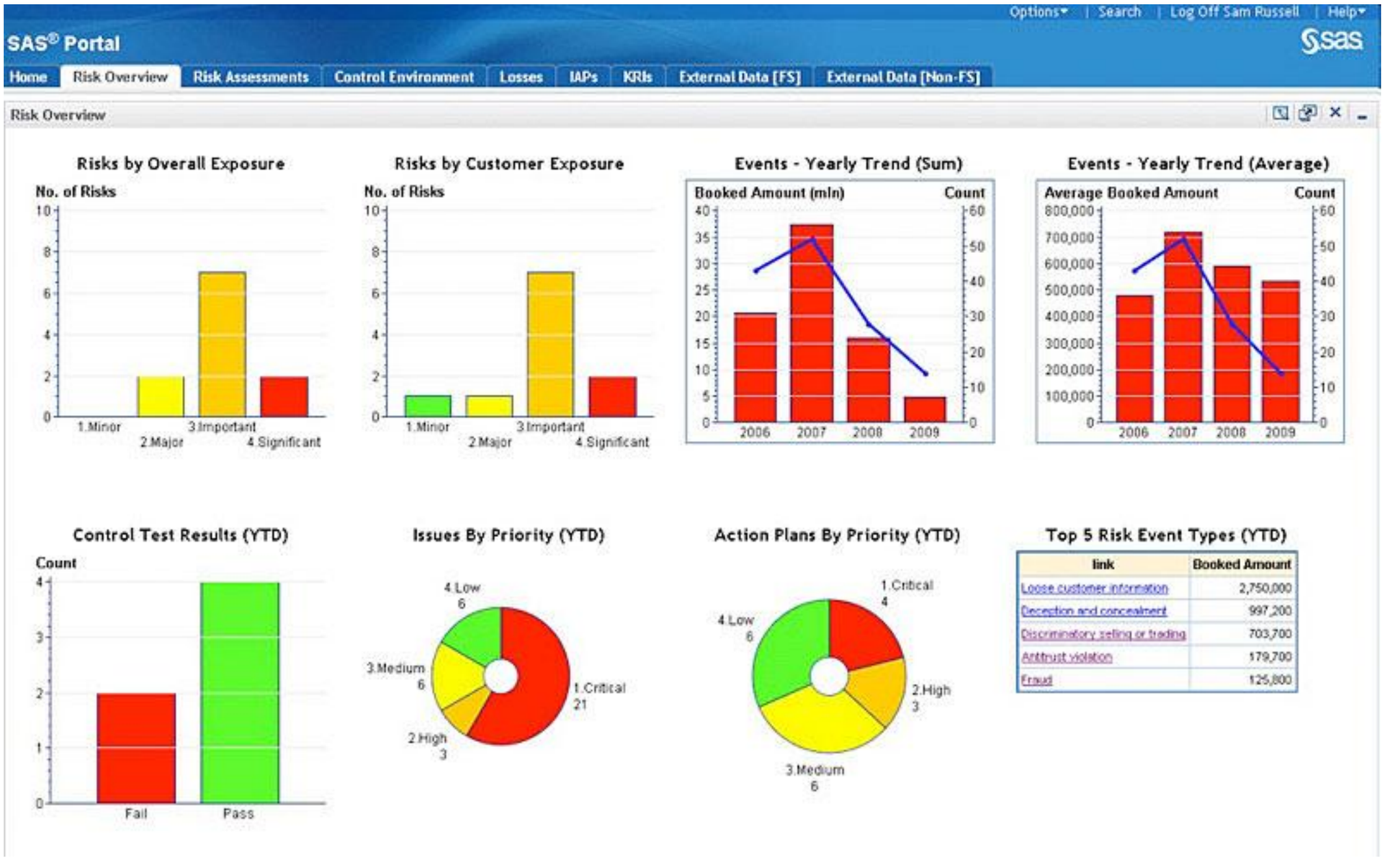
Мошеннические операции



Хищение продукции, манипуляции в технологических и информационных системах учета, искажение финансовой отчетности и т. д.

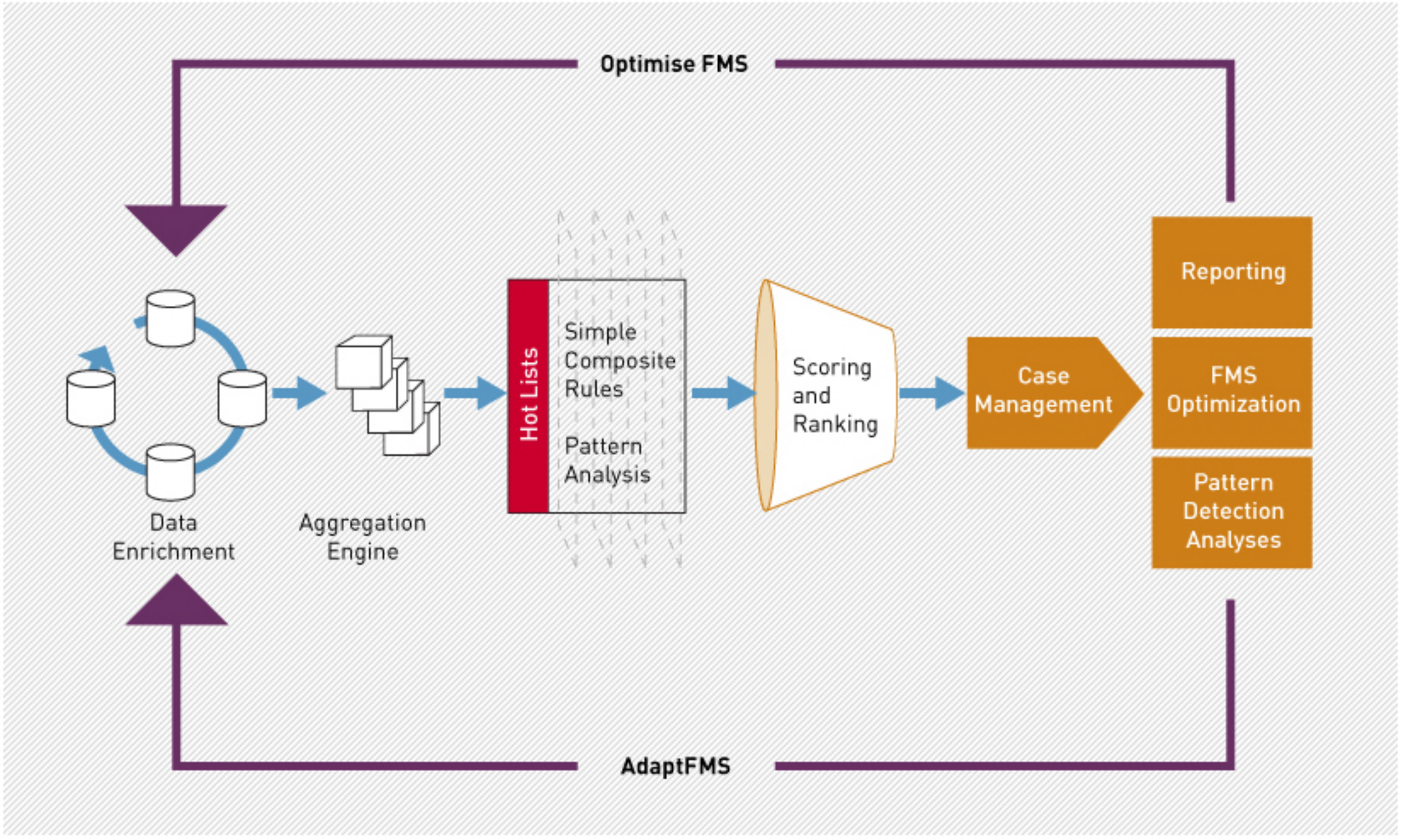
Мошеннические операции

RISSPA
be professional



Риск-менеджмент и фрод-менеджмент системы

Мошеннические операции



Системы мониторинга и анализа событий

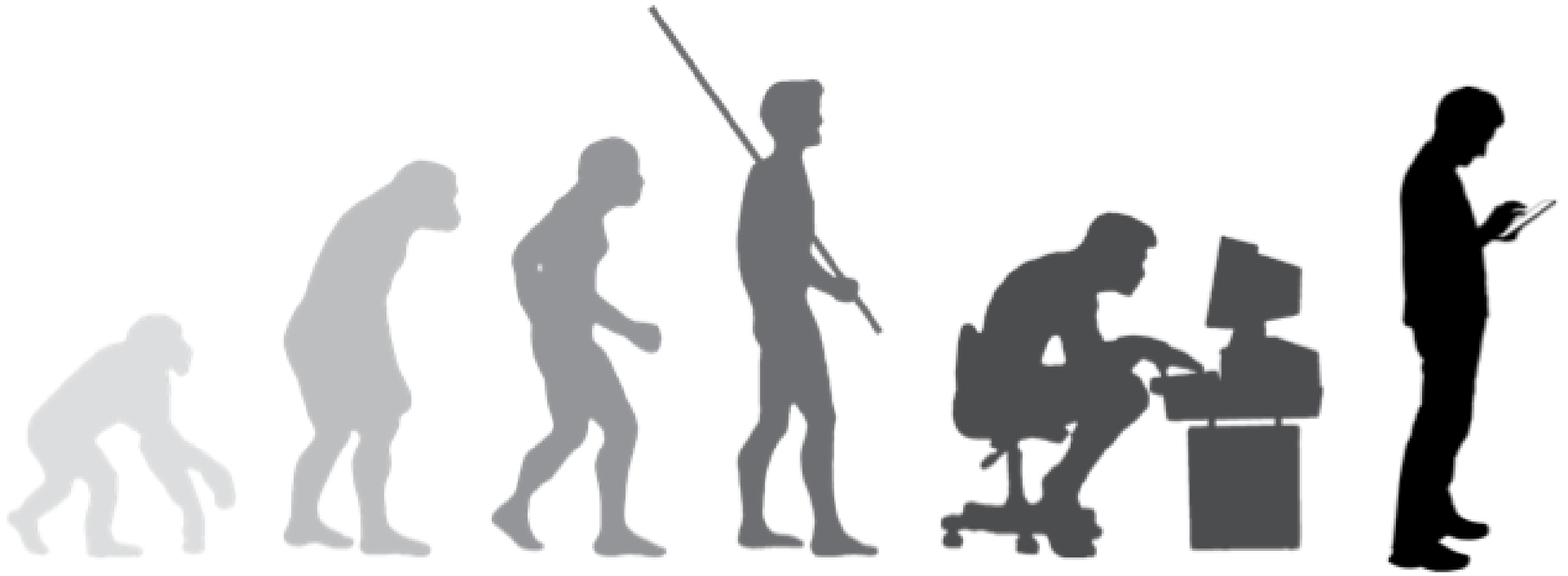
Мошеннические операции

Административные меры

Мотивация персонала

Мобильные устройства

RISSPA
be professional



«Консьюмеризация будет самым значительным трендом,
влияющим на IT в ближайшие 10 лет»

Gartner

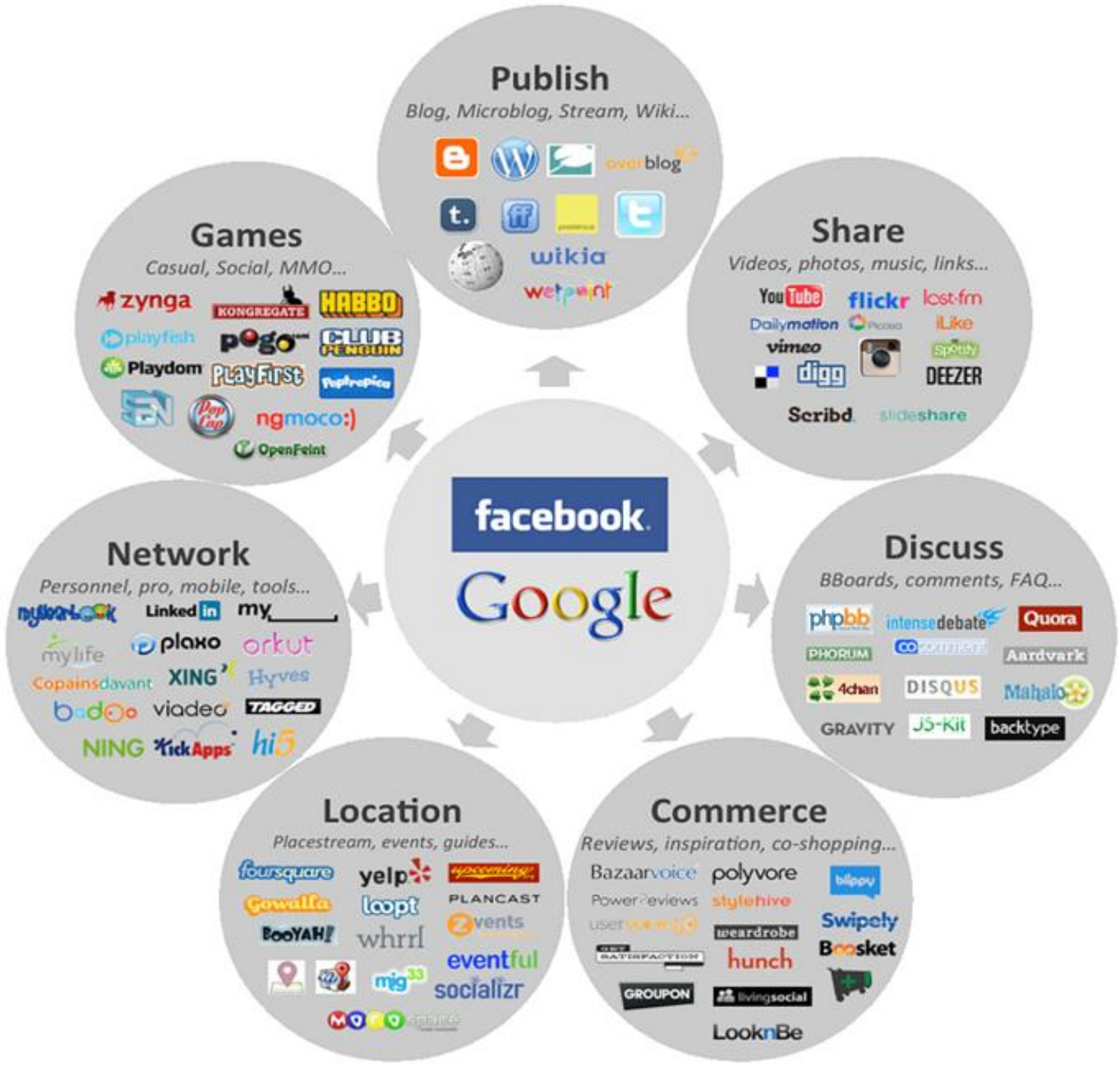
Почему выбирает потребитель?

RISSPA
be professional

iPad + Bluetooth Keyboard + Bluetooth Mouse = Desktop iPad computer?

Почему выбирает потребитель?

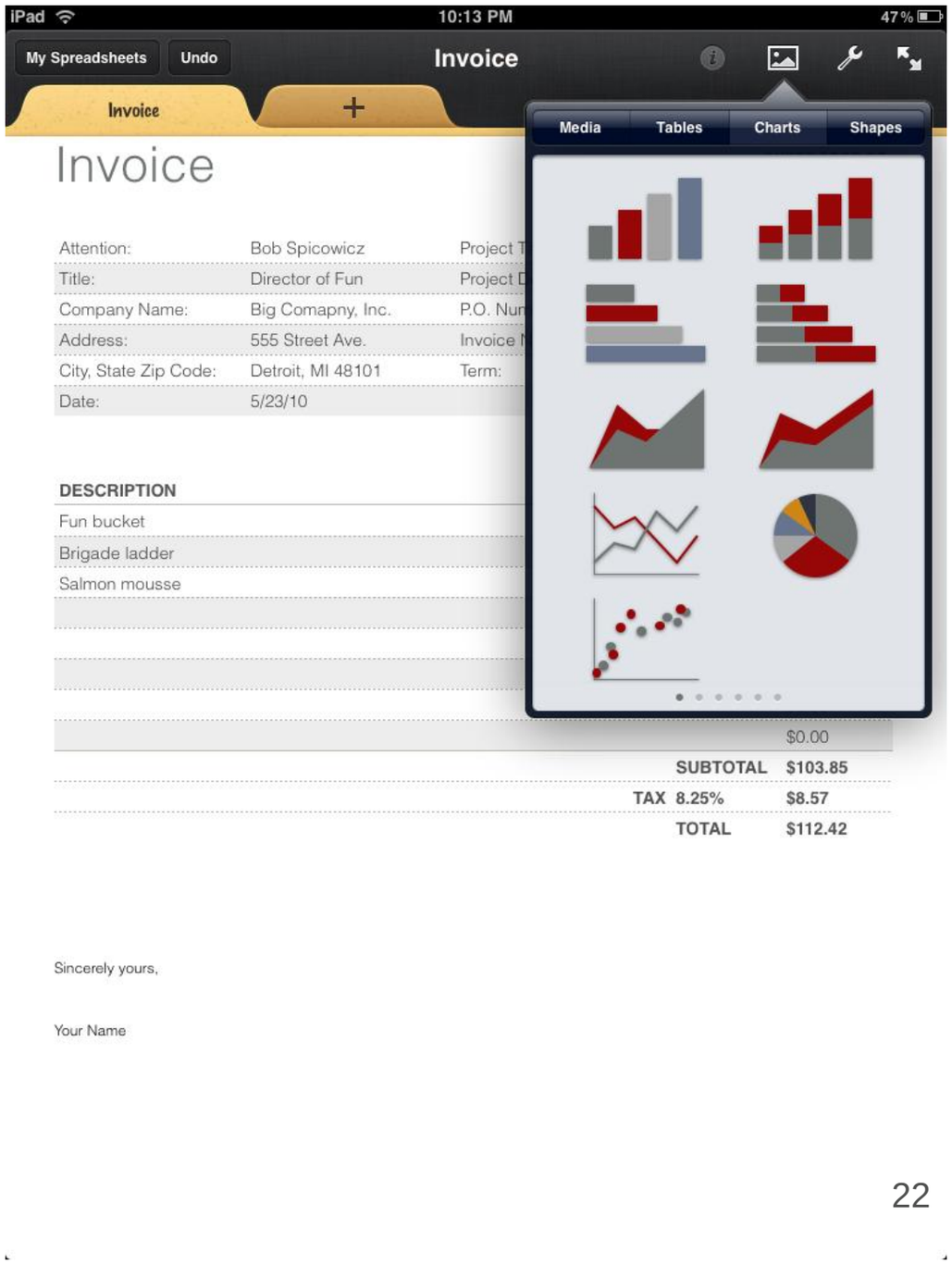
RISSPA
be professional



Почему выбирает бизнес?

RISSPA
be professional

- Снижение затрат
- Удобство
- Постоянная доступность сотрудников
- Повышение эффективности бизнеса
- Мотивация сотрудников
- И еще раз снижение затрат…



Основные риски

Утечка корпоративных данных

•Теперь они хранятся на личных устройствах сотрудников

•Использование недоверенных сервисов хранения и передачи данных (Dropbox, iCloud, etc.)

Кража или потеря устройства

Вредоносное программное обеспечение

Основное опасение – потеря контроля над данными

Как защититься?

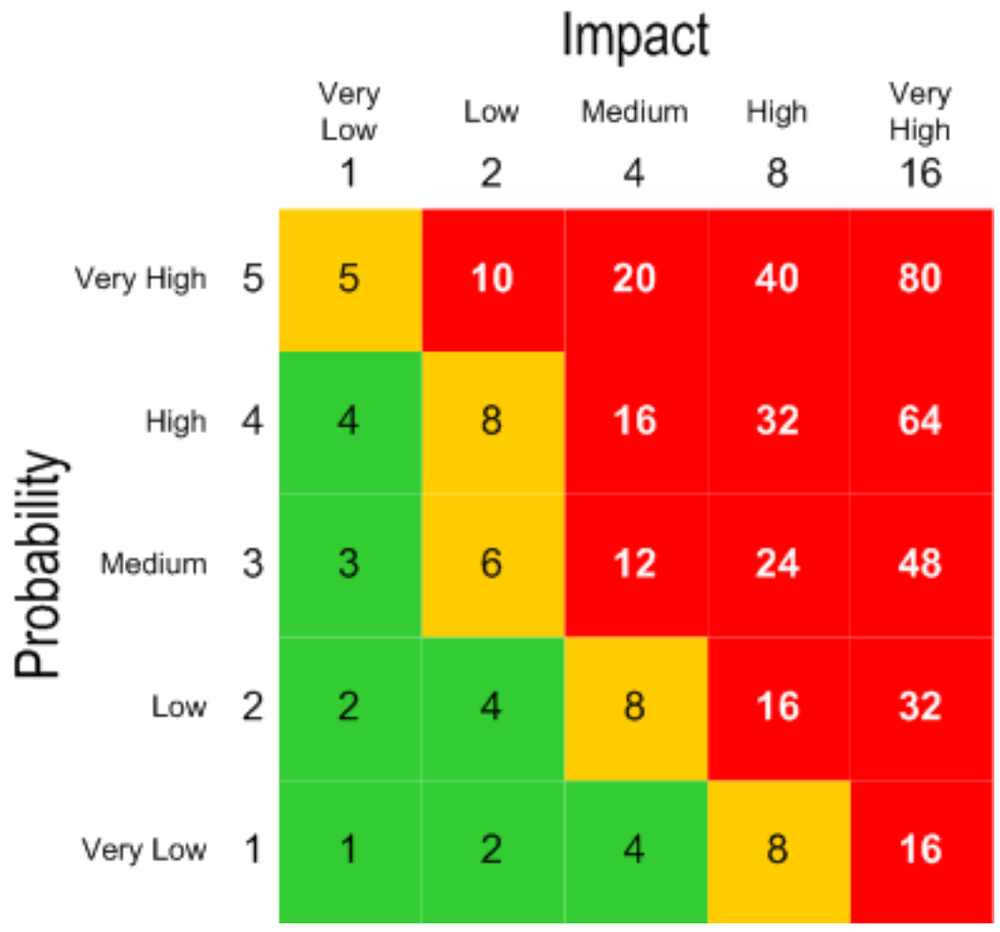
RISSPA
be professional

- Классификация данных, оценка рисков, business value
- Выбор надежной мобильной платформы, настройка политик
- Использование специальных систем управления устройствами
- Защищенные сервисы и мобильные клиенты
- Обучение сотрудников и аудиты защищенности

Как защититься?

RISSPA
be professional

Классификация данных



Оценка рисков

Как защититься?

RISSPA
be professional

Выбор платформы зависит от различных факторов, таких как корпоративные стандарты, наличие мобильных клиентов и др.

Как защититься?

RISSPA
be professional

Настройка политик:

- Состав, длина пароля и срок жизни;
- Защищенный сетевой доступ;
- Удаленное управление доступом;
- Разрешенные/запрещенные приложения;
- Уничтожение данных;
- И другие.

Примеры руководств:
iOS - http://www.dsd.gov.au/publications/iOS_Hardening_Guide.pdf
Android - http://www.sans.org/reading_room/whitepapers/sysadmin/securely-deploying-android-devices_33799
Blackberry - http://www.dsd.gov.au/infosec/epl/view_document.php?document_id=ODE3IyMjMjAzLjYuMTE0LjQ=

Как защититься?

RISSPA
be professional

Решения MDM:

•Мультиплатформенность

•Управляемость

•Интеграция с корпоративной инфраструктурой безопасности, в том числе с центрами сертификации

•Мобильный или тонкий клиент

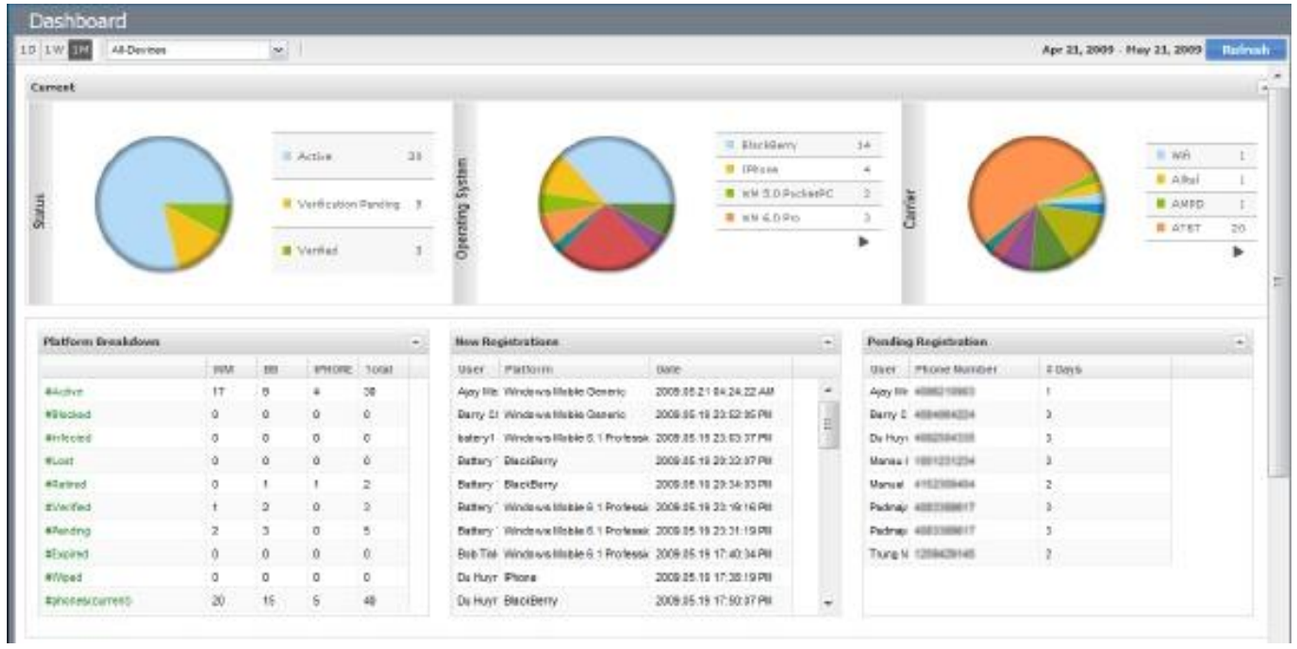
•Единые политики безопасности

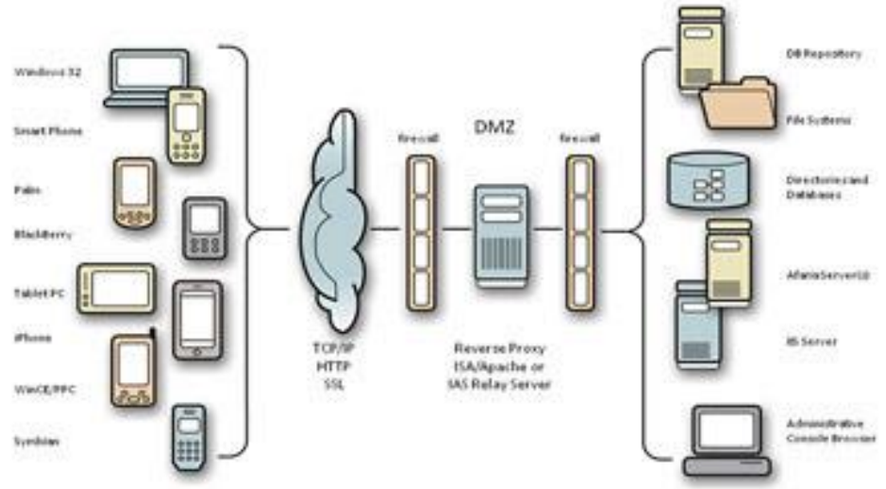
•Дополнительные элементы контроля

•Самообслуживание пользователей

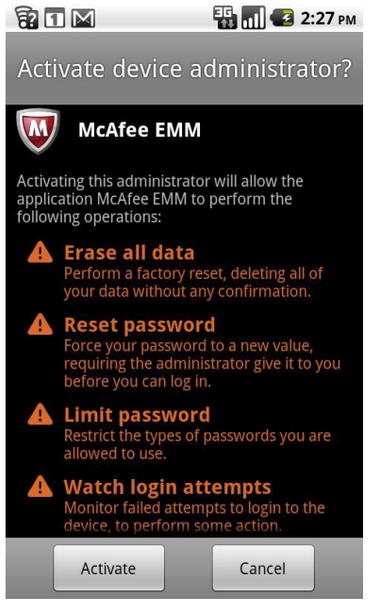
Как защититься?

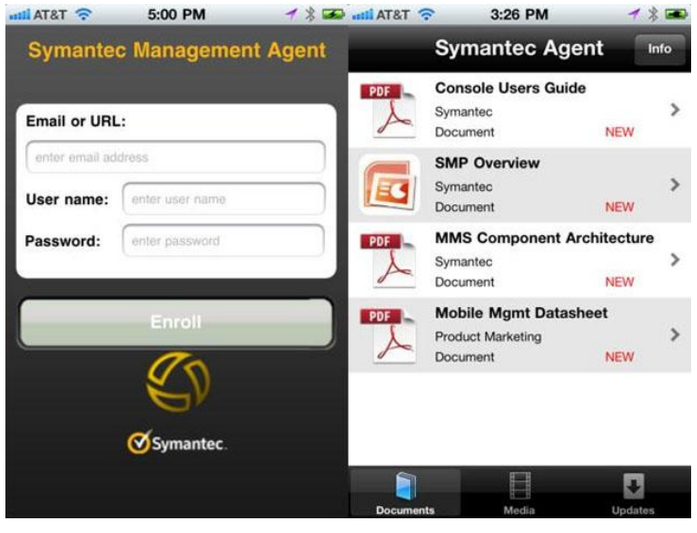
RISSPA
be professional





Zoom





Для примера, сравнительный обзор решений MDM - http://www.solotablet.it/blog/approfondimenti/mobile-device-management

Как защититься?

RISSPA
be professional

Специализированные сервисы и мобильные клиенты часто содержат достойные средства защиты

Как защититься?

RISSPA
be professional

Обучение пользователей

Аудит защищенности

Как защититься?

RISSPA
be professional

Дополнительные материалы:

Sophos Webcast on Android Security:
http://nakedsecurity.sophos.com/2012/01/22/sscc-80-mobile-security-podcast-with-vanja-svajcer/

5 Ways to Protect Your Mobile Apps:
http://www.cio.com/article/683229/Mobile_App_Security_5_Ways_to_Protect_Your_Smartphone

iOS Security Overview:
http://images.apple.com/iphone/business/docs/iOS_Security.pdf

SANS Mobile Security Policy Templates:
http://www.sans.org/security-resources/policies/mobile.php

Mobile Device Forensics:
http://www.sans.org/reading_room/whitepapers/forensics/mobile-device-forensics_32888

Mobile Device Security:
http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/7-051909-new-technologies-mobile-devices.pdf

+ Google, Yandex, спросить меня… ☺

Что такое RISSPA?

RISSPA
be professional

Контакты и общение

Продвижение идей ИБ

Членство и участие в семинарах бесплатно

Регулярные очные и онлайн семинары

Ассоциация профессионалов в области информационной безопасности (Russian Information Security Systems Professional Association) Создана в июне 2006 года

Формирование сообщества профессионалов в области ИБ

Обмен опытом

Повышение уровня знаний специалистов ИБ

Обсуждение актуальных проблем ИБ

cloud security alliance SM

(ISC)² International Standard for Information Security

Мы в сетях

RISSPA
be professional

www.RISSPA.ru