IBM BusinessConnect

соединяя бизнес и технологии

20 марта 2015 г | Москва

BusinessConnect
соединяя бизнес и технологии

Обеспечение интеллектуальной ИТ-безопасности и защита данных в контексте потребностей бизнеса сегодня

BusinessConnect
соединяя бизнес и технологии

Бакшинский Олег

Руководитель направления систем управления ИБ

IBM Россия/СНГ

IBM

BusinessConnect
соединяя бизнес и технологии

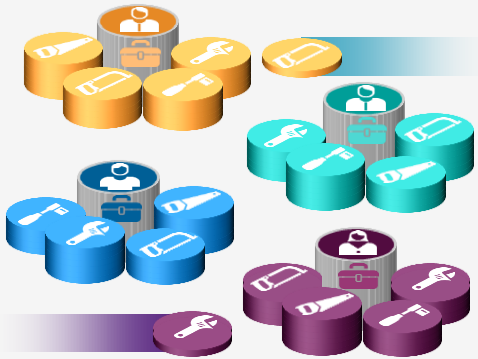
Потребности бизнеса сегодня

ПРОБЛЕМЫ СЕГОДНЯ И СТРАТЕГИЯ IBM

Все больше атак

- Изощренные методы атак
- Исчезающий периметр
- Использование уязвимостей в системах безопасности

Все сложнее защищать



- Постоянно изменяющаяся инфраструктура
- Много продуктов от разных вендоров; дорого настраивать и управлять
- Неадекватные и неэффективные инструменты

Все меньше ресурсов

- Недостаток специалистов ИБ
- Слишком много данных при ограниченных ресурсах и навыках управления ими
- Управление и мониторинг – требования регуляторов

ПОСТОЯННЫЙ МОНИТОРИНГ СОБЫТИЙ ИБ

Единая интеллектуальная платформа мониторинга и анализа

Предсказывать и приоритезировать слабые элементы системы ИБ до того, как это сделают злоумышленники

Аналитика до атаки

Оценка рисков и уязвимостей

Определять активности и аномалии в отличие от нормального поведения

Аналитика атаки в реальном времени

Управление событиями ИБ

ВЫЯВЛЯТЬ, ОТСЛЕЖИВАТЬ, ЗАКРЫВАТЬ

Расследование инцидентов после атаки

Уменьшить время на полное расследование того, что и когда произошло

Полное восстановление картины инцидентов

Быстрая интеграция

Быстро охватить много областей ИБ защищая будущее

Интеграция решений ИБ на одной платформе

Сервис реагирования

Подготовиться и противостоять атакам эффективнее

IBM Emergency Response Services

BusinessConnect
соединяя бизнес и технологии

Обеспечение ИТ-безопасности и защита данных

IBM

Интеллектуально

Интегрированно

Автоматизированно

ИНТЕЛЛЕКТУАЛЬНОЕ ОПРЕДЕЛЕНИЕ

INTELLIGENT

Устройства ИБ

Сервера и мейнфреймы

Сетевая и виртуальная среда

Активности БД

Работа приложений

Конфигурации устройств

Уязвимости и угрозы

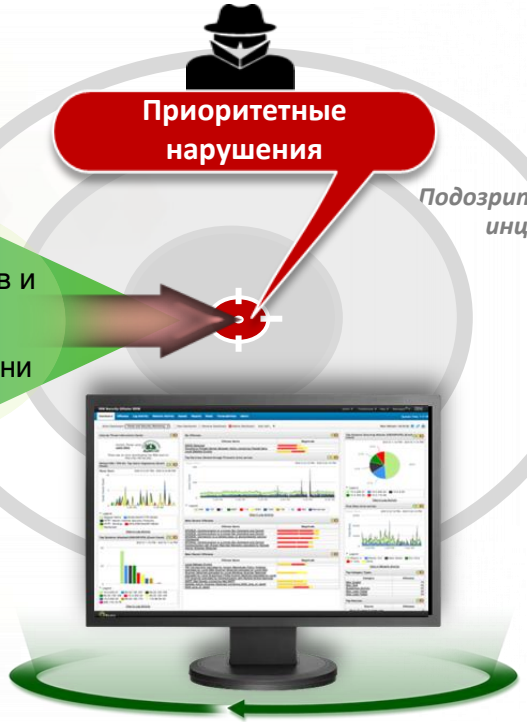
Пользователи и учетки

Глобальные базы угроз

Авто Определение Нарушения

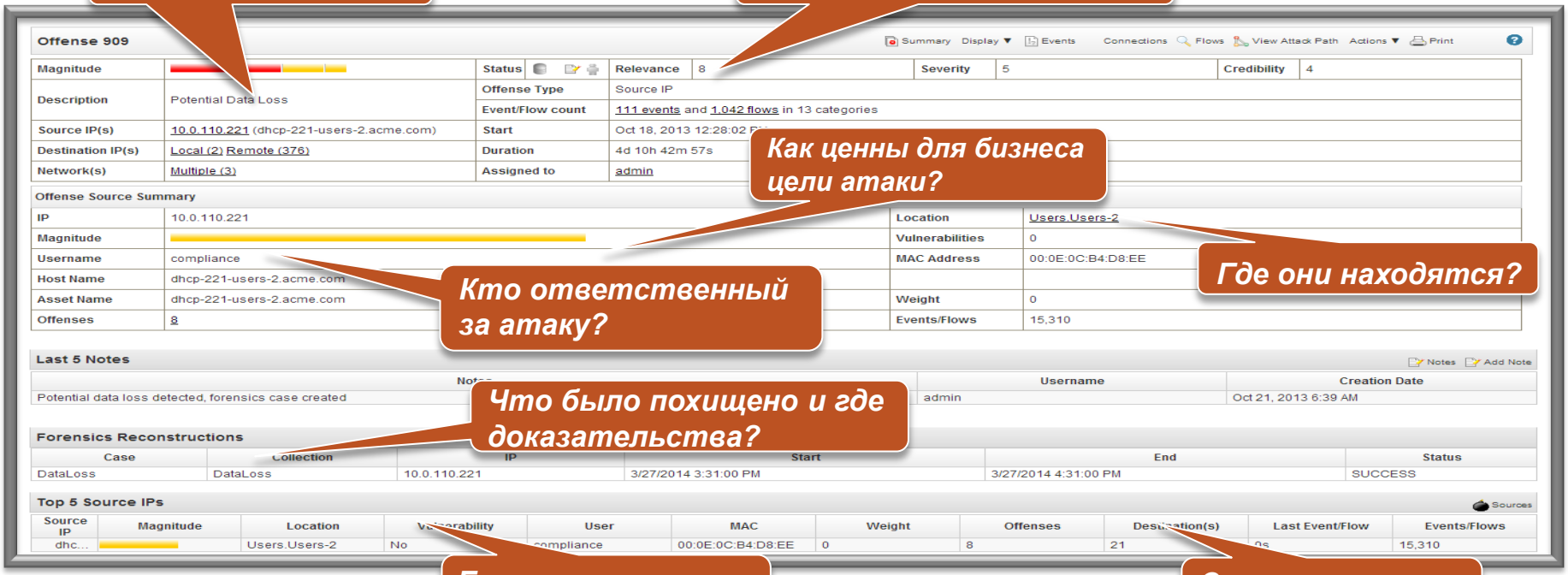
- Сбор, хранение и анализ данных
- Встроенная классификация
- Авто определение источников, сервисов и пользователей и их профилирование
- Корреляция событий в реальном времени
- Определение аномалий активностей
- Определение инцидентов из коробки

Встроенный интеллект

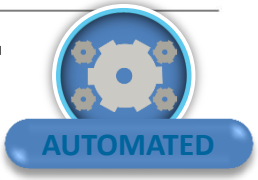


БЫСТРЫЕ ОТВЕТЫ ЧЕРЕЗ ИНТЕГРАЦИЮ

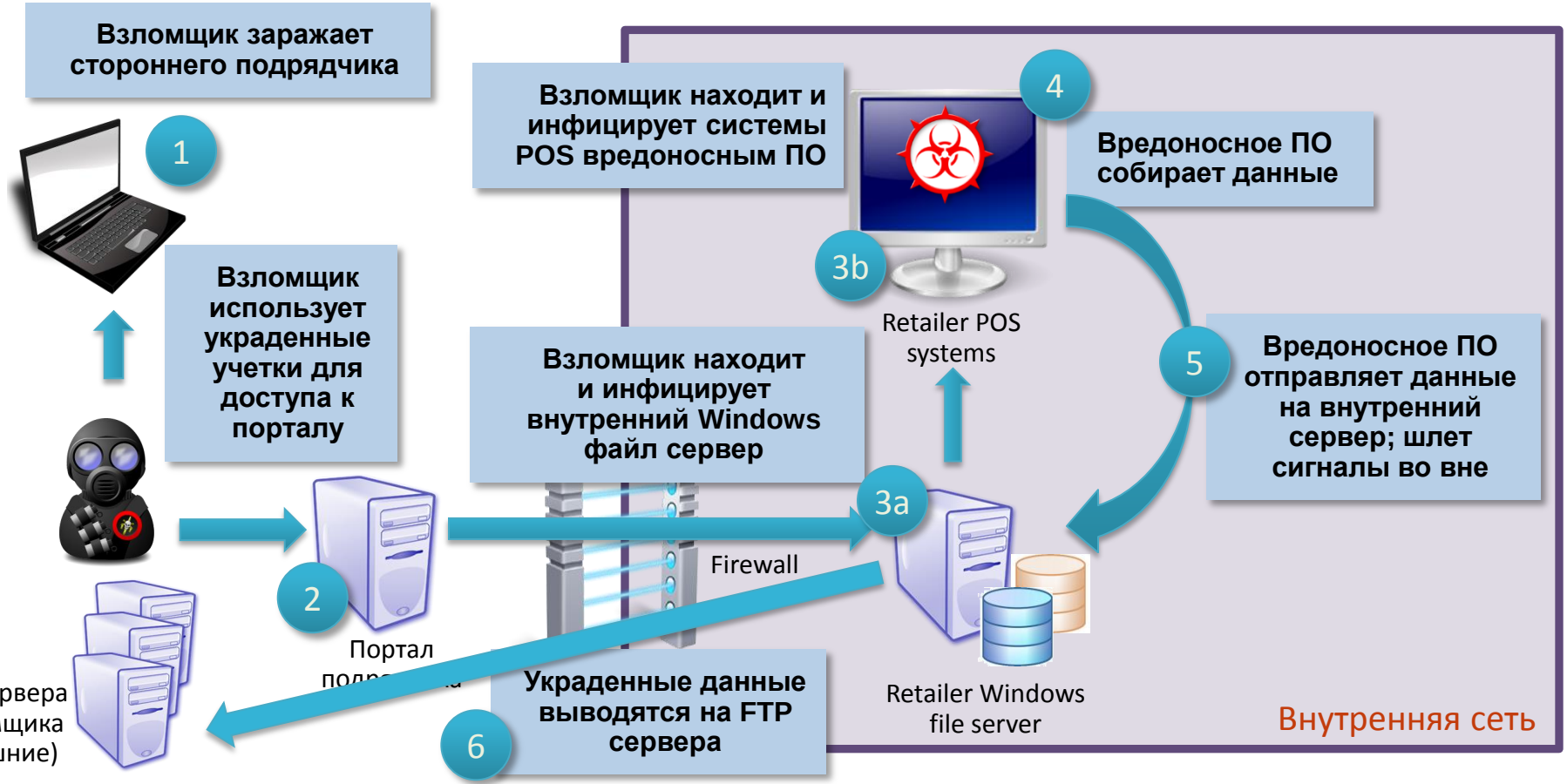
INTEGRATED

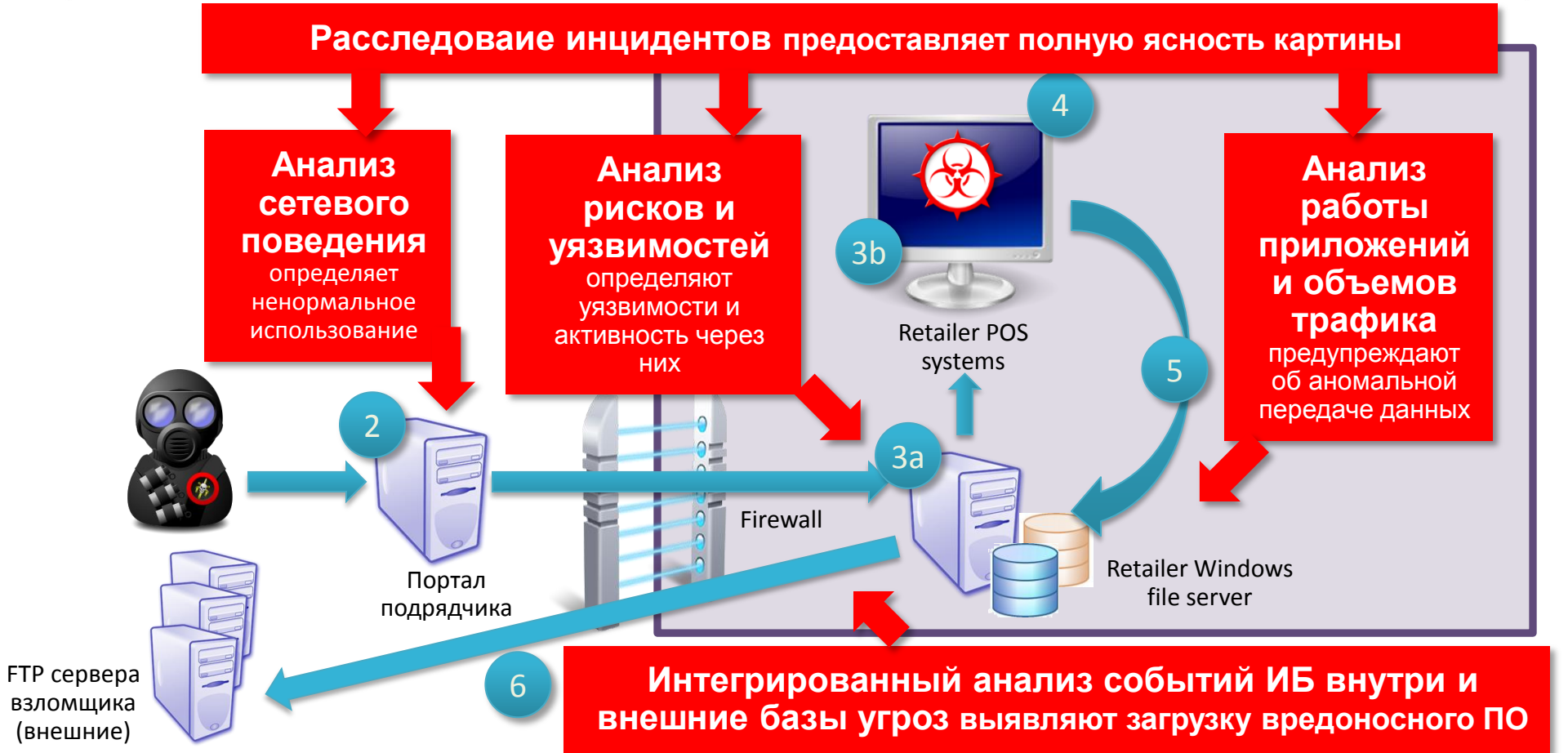


ПРОСТОТА И НЕМЕДЛЕННЫЙ РЕЗУЛЬТАТ



Что это дает заказчикам?


Взломщик заражает стороннего подрядчика
1
Взломщик использует украденные учетки для доступа к порталу
2
Портал
Взломщик находит и инфицирует системы POS вредоносным ПО
4
Вредоносное ПО собирает данные
3b
Retailer POS systems
5
Вредоносное ПО отправляет данные на внутренний сервер; шлет сигналы во вне
Взломщик находит и инфицирует внутренний Windows файл сервер
3a
Firewall
Retailer Windows file server
Внутренняя сеть
Украденные данные выводятся на FTP сервера
6
FTP сервера взломщика (внешние)


Расследоваие инцидентов предоставляет полную ясность картины
Анализ сетевого поведения
определяет ненормальное использование
Анализ рисков и уязвимостей
определяют уязвимости и активность через них
Анализ работы приложений и объемов трафика
предупреждают об аномальной передаче данных
4
3b
Retailer POS systems
5
2
Портал подрядчика
3a
Firewall
Retailer Windows file server
FTP сервера взломщика (внешние)
6
Интегрированный анализ событий ИБ внутри и внешние базы угроз выявляют загрузку вредоносного ПО

ПРИМЕР КЛИЕНТА

Оптимизация анализа угроз

Анализируется

2 млрд.

событий ИБ в день для выявления

20-25

потенциальных нарушений для расследования

Задачи

- Уменьшить огромное количество событий для расследования важных
- Автоматизировать процесс анализа событий ИБ

Комплексное решение на платформе IBM Security Solutions

Комбинированный анализ архивных данных с событиями в реальном времени создает общую картину выявляя нехарактерные активности незаметные для человека и тут же блокирует подозрительный траффик

BusinessConnect
соединяя бизнес и технологии

Подводим итоги

ОБЗОР РЕЗУЛЬТАТОВ 2014

- Рост Security Intelligence более 35%
- Новые решения для расследования инцидентов
- Более 500 **новых** заказчиков из числа крупнейших компаний по всему миру

- No 1 по оценке ведущих аналитиков
- Стратегия IBM Security Intelligence приносит результаты

ИТОГИ

Лидер в Security Intelligence, управлении уязвимостями и расследовании инцидентов

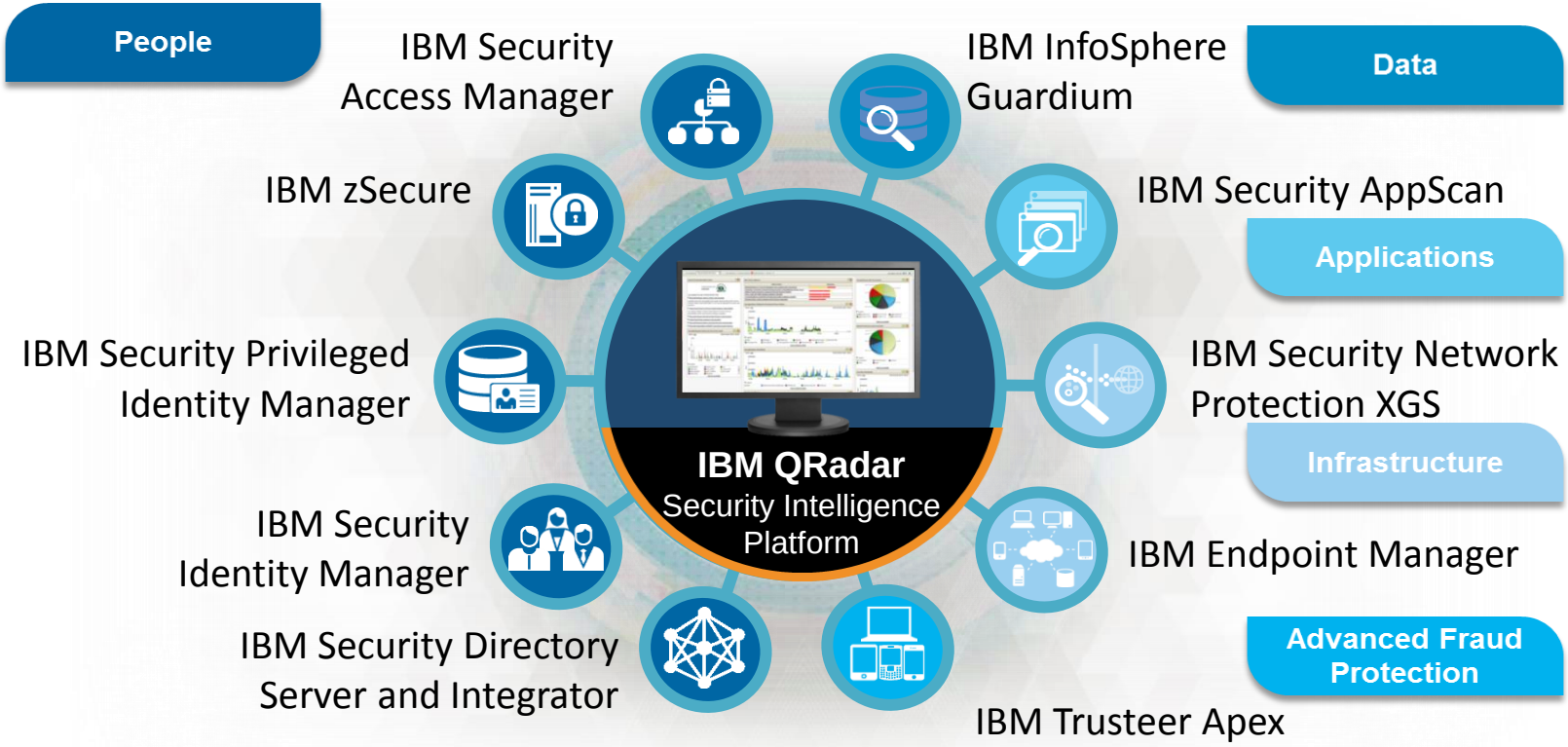
- Нас отличает быстрый результат от внедрения, единая интегрированная платформа и автоматизация
- Соответствие нормативам регуляторов и максимальная визуализация картины ИБ и определение угроз

Новые возможности доступны уже сегодня

- Глобализация, Расследование инцидентов, Расширенный поиск по событиям ИБ, Поддержка облачных решений, Выявление новых угроз в реальном времени

IBM сегодня представляет действительно интегрированное решение Security Intelligence

ЦЕНТР ИНТЕГРАЦИИ РЕШЕНИЙ IBM SECURITY



BusinessConnect
соединяя бизнес и технологии

Спасибо