19 сентября 2017

Облачные сервисы безопасности

Алексей Смирнов
Менеджер по развитию бизнеса

orange™ Business Services

Кибератаки и современные угрозы

У хакеров и злоумышленников есть много причин и методов/инструментов для проведения успешных атак, которые напрямую влияют на бизнес компаний

Мотивация	Методы	Результат
▪ Кража корпоративных или персональных данных ▪ Бизнес разведка ▪ Получение конкурентного преимущества ▪ Получение политического преимущества ▪ Социальный или политический хактивизм	▪ (Spear) Phishing кампании ▪ Эксплуатирование уязвимостей ▪ Использование скрытых каналов ▪ Инсайдеры и социальная инженерия ▪ Вирусы и вредоносное ПО ▪ DDoS атаки ▪ Advanced Persistent Threat и т.д.	▪ Снижение финансовых показателей ▪ Снижение доли рынка для компании ▪ Дополнительные затраты на устранение последствий и расследования ▪ Снижение доверия со стороны клиентов и партнеров ▪ Снижение стоимости бренда и привлекательности компании для инвесторов

Комплексный подход

Уровни защиты	Участники	Основные технологии
Предсказательный подход	Исследователи ИБ	CERT Анализ вредоносного ПО Анализ аномалий
Проактивный подход	**Cyber SOC** аналитики	Реагирование на инциденты Корреляция событий Наблюдение и обнаружение
Реактивный подход	**SOC** IT и сетевые специалисты	Управление уч. данными Безопасный периметр Защита устройств
Базовый уровень защиты	Все сотрудники компании	ИБ осведомленность Политики ИБ

Примеры облачных сервисов безопасности

Аутентификация из облака

Описание задачи:

- Retail компания с большим количеством мобильных сотрудников;
- Требуется доступ ко многим ИТ системам внутри сети;
- Необходимо снизить риски НСД за счет использования 2х факторной аутентификации (VPN и WEB порталы).

РЕШЕНИЕ И ВЫВОДЫ:

- Большая часть инфраструктуры уже реализована и состоит из большого количества продуктов безопасности
- Централизованная и быстро масштабируемая система для 2х факторнной аутентификации

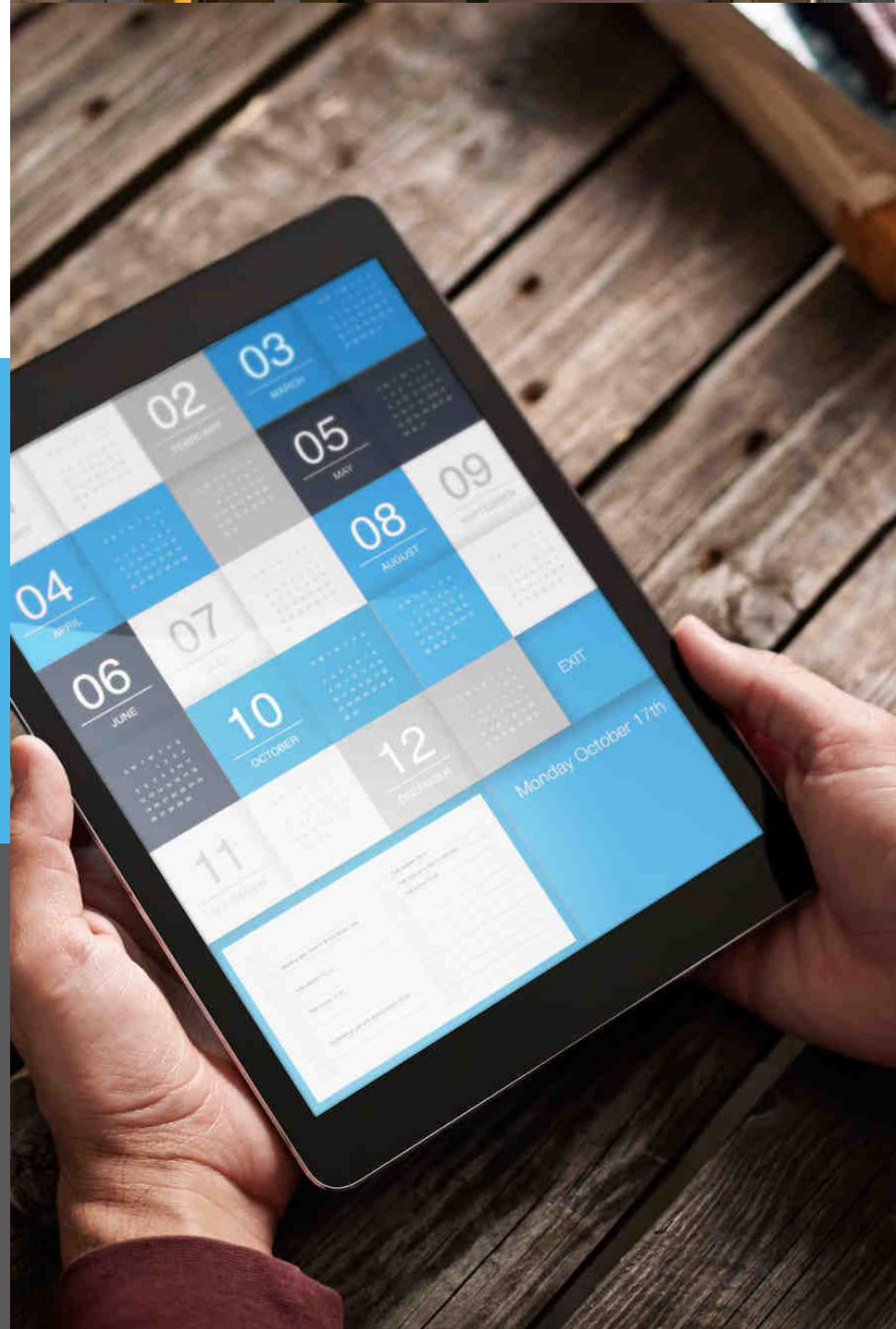
Безопасность мобильных устройств

ЗАДАЧИ ДЛЯ БИЗНЕСА:

- Снижение затрат за счет внедрения удаленной работы;
- Снижение риска утечки конфиденциальных данных через неконтролируемые личные смартфоны;
- Обеспечить доступ ко всем ИТ системам, необходимым для работы

РЕЗУЛЬТАТ:

- Отсутствие капитальных затрат на инфраструктуру;
- Быстрое внедрение и масштабирование;
- Отказоустойчивость и поддержка 24x7x365
- Снижение затрат на ИТ



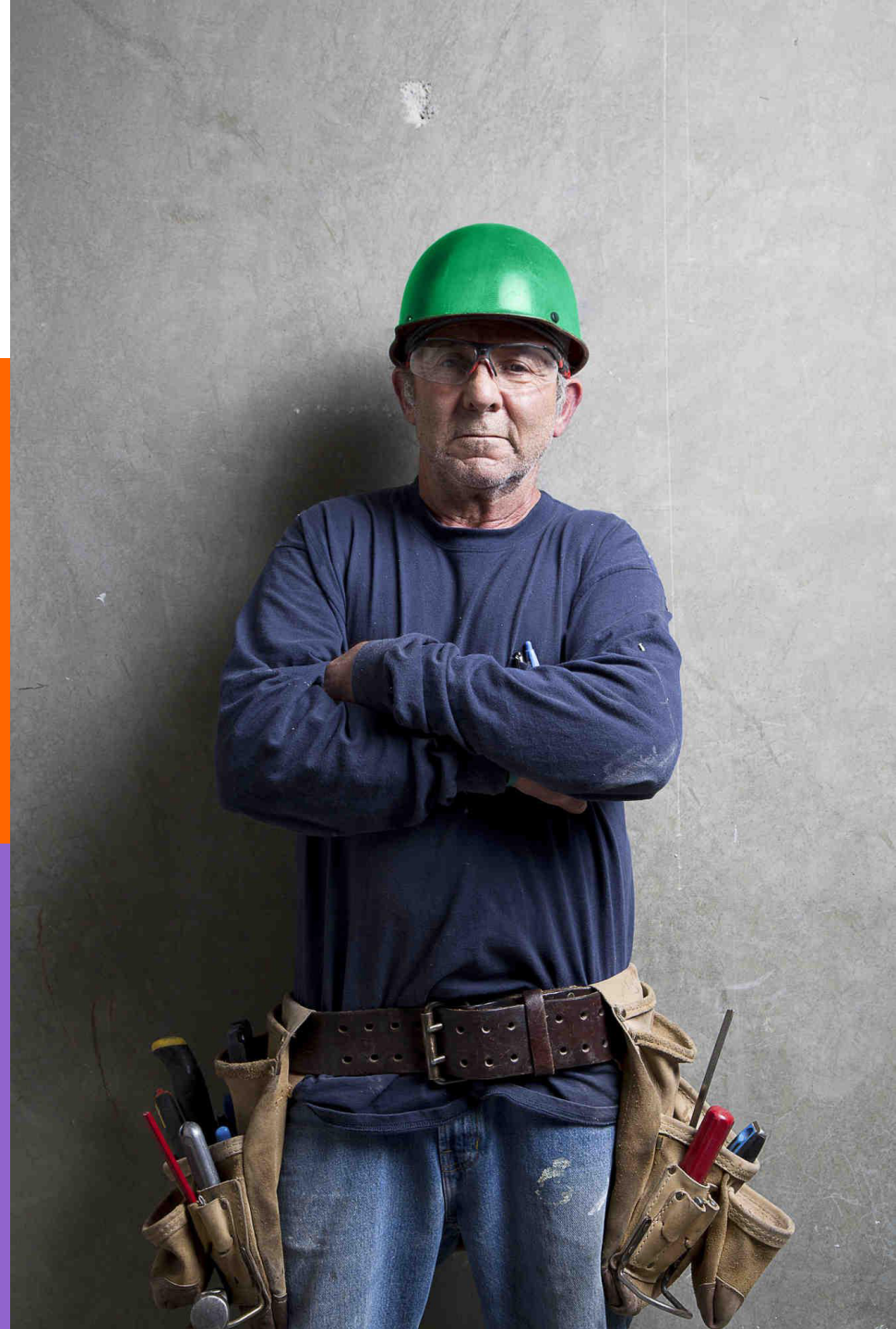
Облачный межсетевой экран

Эволюция WAN сети:

- 2008 год – сеть построена на частных каналах связи (MPLS)
- 2010 год – Internet VPN в качестве резерва + балансировка нагрузки)
- 2014 год – гибридное IT – необходим локальный выход в интернет на каждом сайте

РЕШЕНИЕ И ВЫВОДЫ:

- Централизация политик безопасности, за счет использования «облачного межсетевого экрана»
- Интернет трафик перенаправляется в ближайший ЦОД
- Высокая доступность, минимальная сетевая задержка, высокий уровень безопасности



Guest WiFi

ЗАДАЧИ:

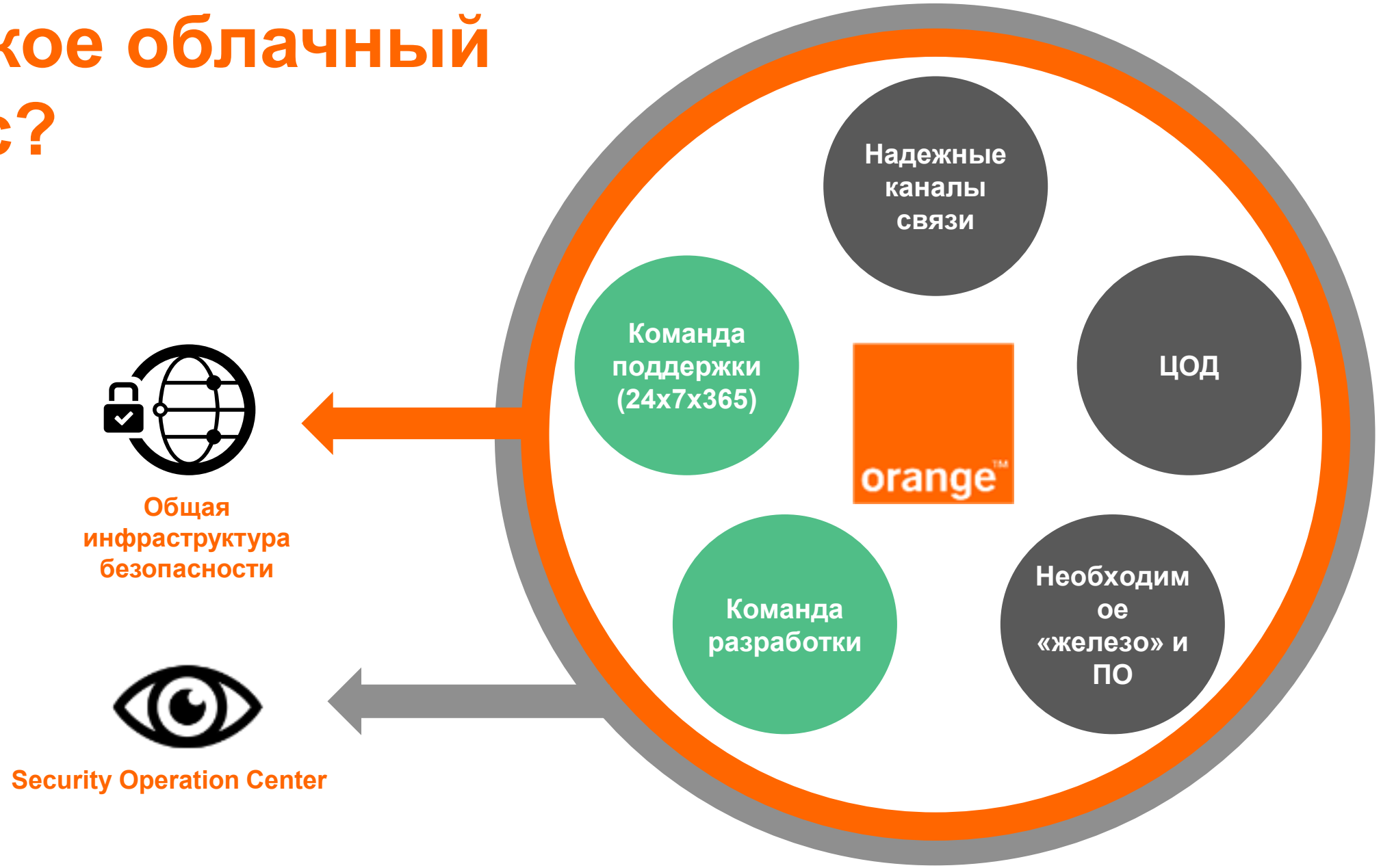
- Retail компания, необходимо обеспечить WiFi Internet для посетителей торгового зала
- Compliance: ПП №758 и ПП №801 – уникальная идентификация пользователя при подключении к публичному WiFi
- Все по OPEX модели, минимум инвестиций

РЕЗУЛЬТАТ:

- Отсутствие капитальных затрат
- Фокусирование ИТ на business critical системах
- Значительное снижение рисков compliance
- Повышение лояльности клиентов, повышение количества потенциальных клиентов

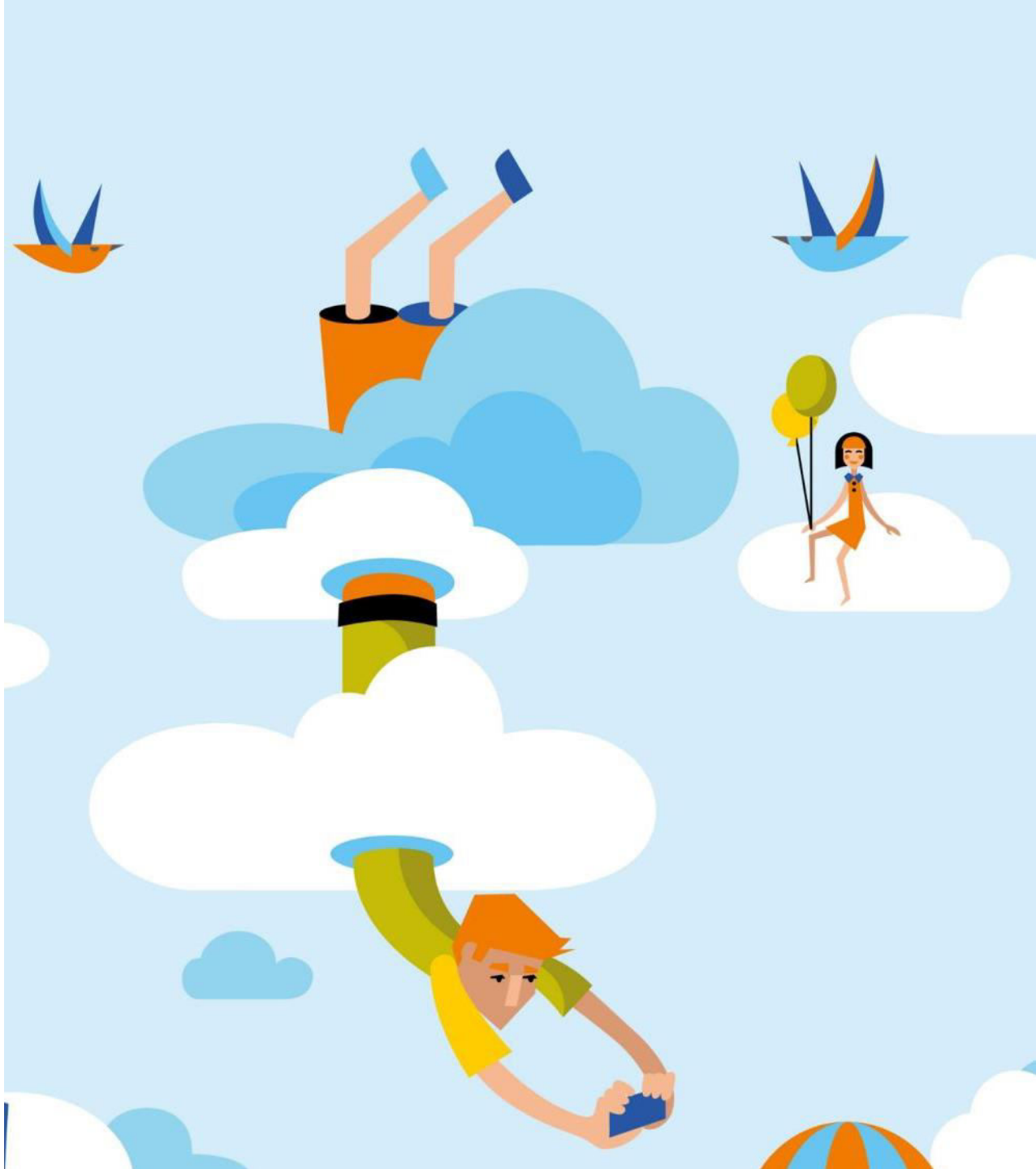
Выбор надежного партнера

Что такое облачный сервис?



Критерии выбора надежного партнера

- **Гибкость** и возможности кастомизации = сильная команда разработчиков
- **Комплексность** = знание большого спектра ИТ технологий
- Общая инфраструктура ИБ и компетенции
- SoC, сертификации в области безопасности (ISO 27001)
- Локальный и глобальный опыт в предоставлении подобных сервисов
- Необходимые лицензии и сертификаты



Спасибо!

orange™ Business Services