



InfoWatch

Доверенная
корпоративная
мобильная
инфраструктура

О ГК InfoWatch

InfoWatch более 15 лет на рынке

Один из крупнейших
ИБ-производителей России

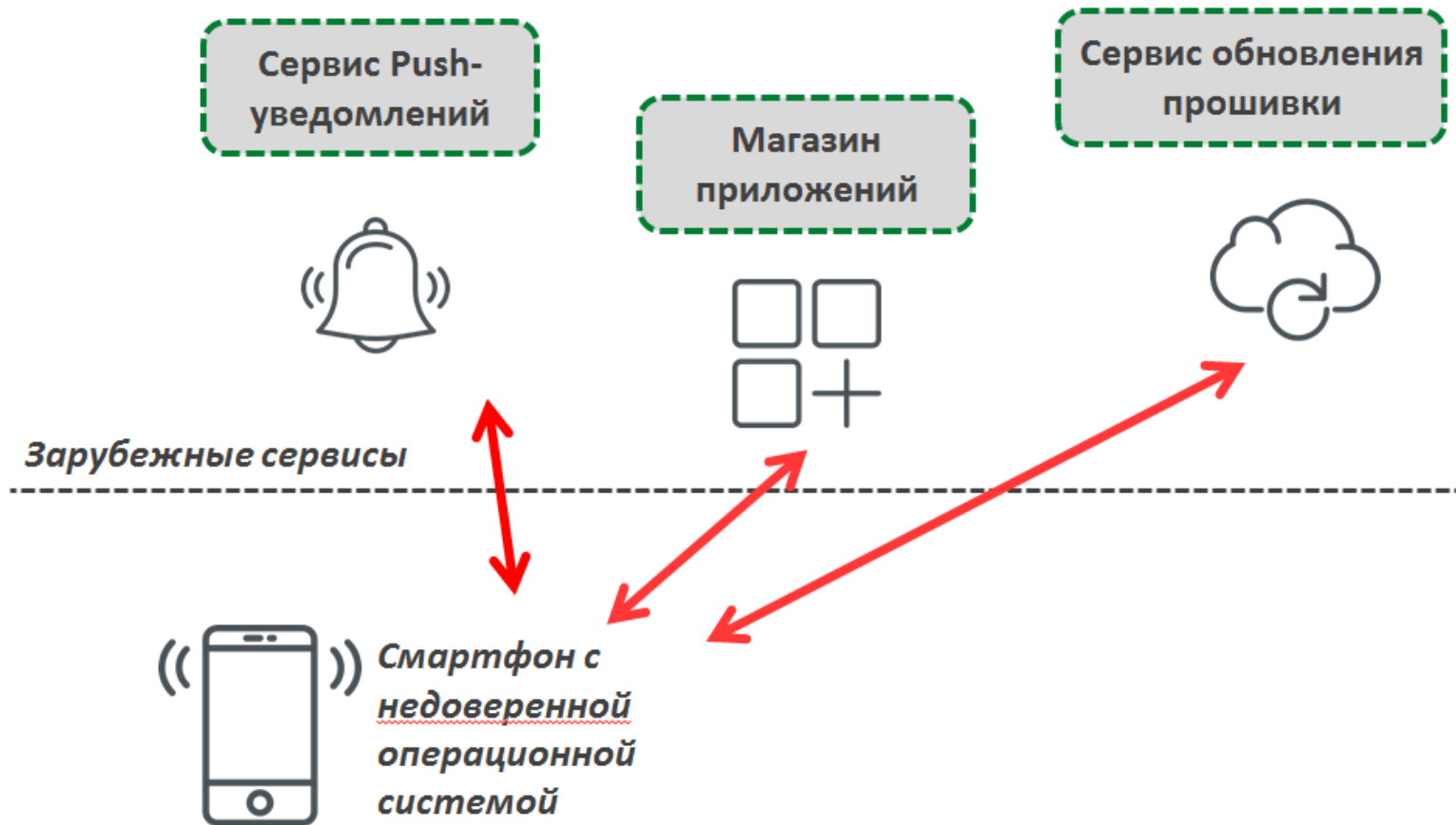
Собственные запатентованные
технологии

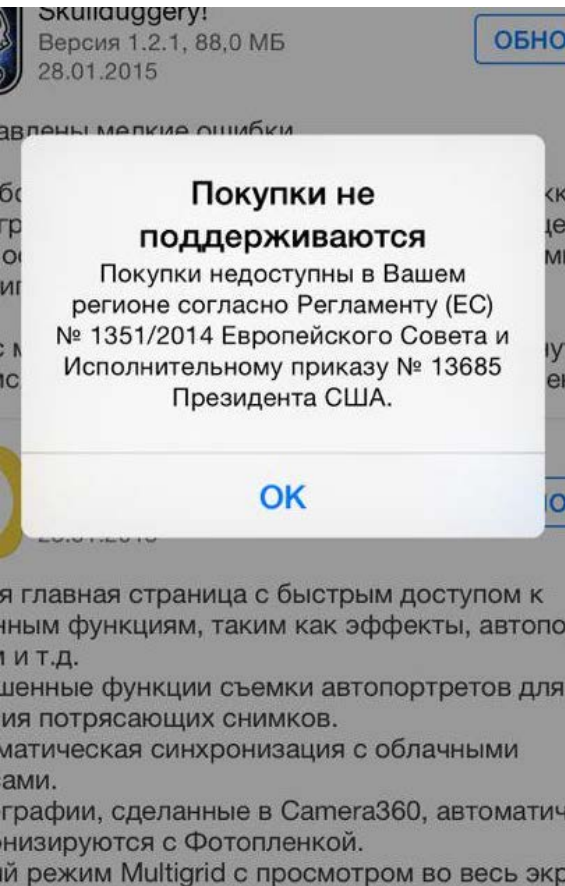
Более полутора тысяч клиентов

Богатый опыт внедрения



Современный мобильный периметр





Утечки обрабатываемых данных

- в результате эксплуатации встроенных программных и аппаратных закладок

Использование сервисов для скрытного получения данных

- видео, аудио, координаты, документы, контакты, звонки и т.д.

Массовый или таргетированный отказ сервисов

- отключение интерфейсов
- ограничение приложений
- полная блокировка устройства

Эдвард Сноуден: *«Управление правительственной связи Великобритании (GCHQ) способно с легкостью взламывать смартфоны без ведома пользователя»*



- **«Мечтательный смурф»** (Dreamy Smurf) – инструмент способный управлять питанием, включая и выключая гаджет без ведома пользователя
- **«Любопытный смурф»** – система управления микрофоном, позволяющая прослушивать все происходящее вокруг, даже когда выключенный телефон лежит в кармане
- **«Смурф-следопыт»** (Tracker Smurf) – механизм высокоточной геолокации в основе которого лежит метод триангуляции по вышкам мобильной связи

Примеры мобильных утечек

Военнослужащий публикует селфи с тегами геолокации, что позволяет точно определить местонахождение подразделения и боевой техники



Офицер загружает карты и другие конфиденциальные документы на личный смартфон, и теряет его

Утечка информации о позициях, численности войск, техническом оснащении подразделений в результате общения в соцсети с подставными пользователями, применяющими методы социальной инженерии



The Famous -
BRITISH WW-II "B2"
SPY RADIO
3,950 €

Как безопасно использовать
смартфон?



INFOWATCH TAIGAPHONE



Модуль мобильной безопасности



INFOWATCH TAIGAPHONE



- ✓ **Модуль InfoWatch Traffic Monitor**
- ✓ **Расширение периметра компании**
- ✓ **Доверенное устройство для сотрудника**
- ✓ **Централизованное управление**



Безопасное **расширение периметра** корпоративной сети

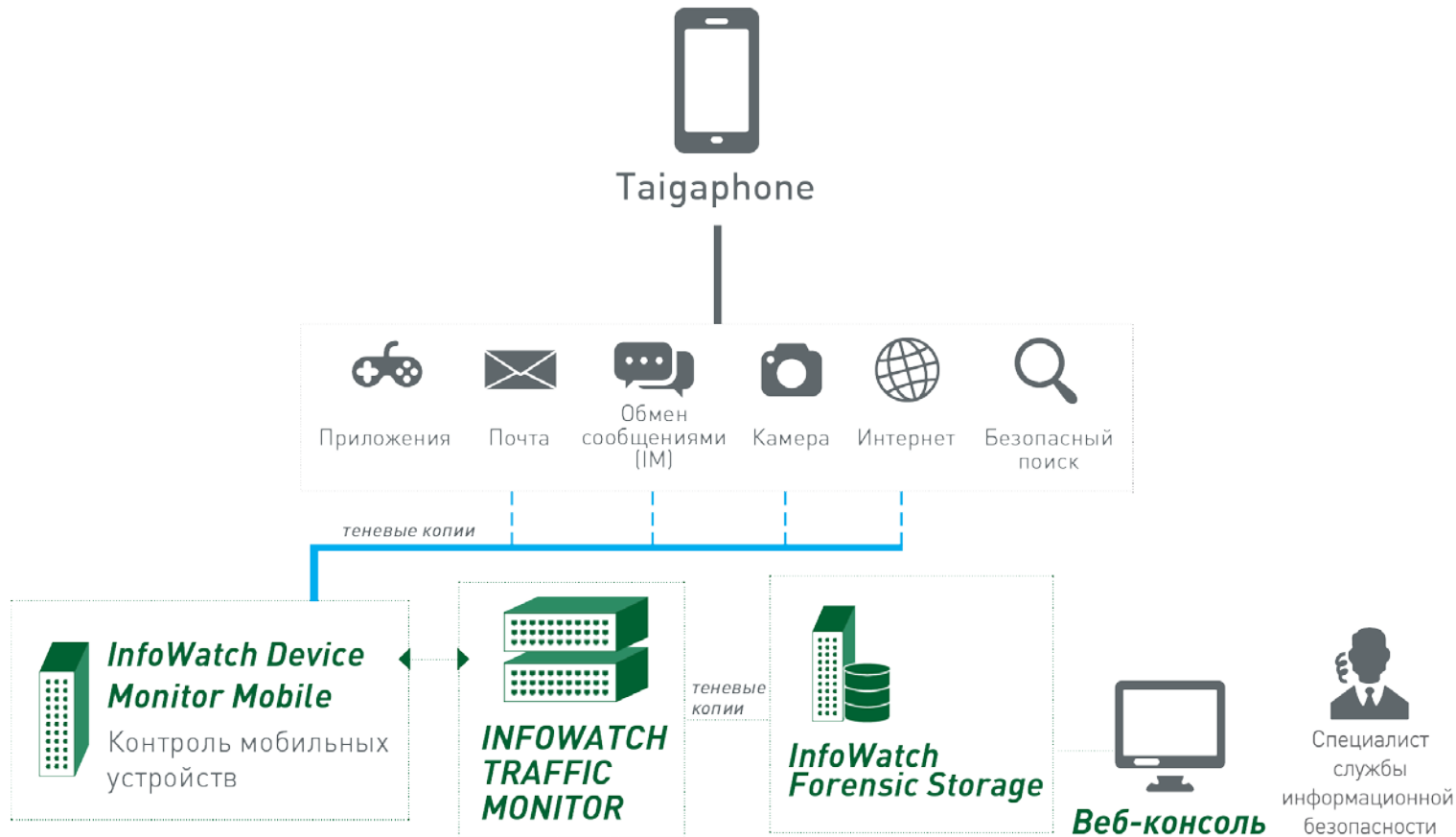
Контроль **каналов коммуникаций** сотрудников на смартфоне

Доверенное устройство для мобильных сотрудников

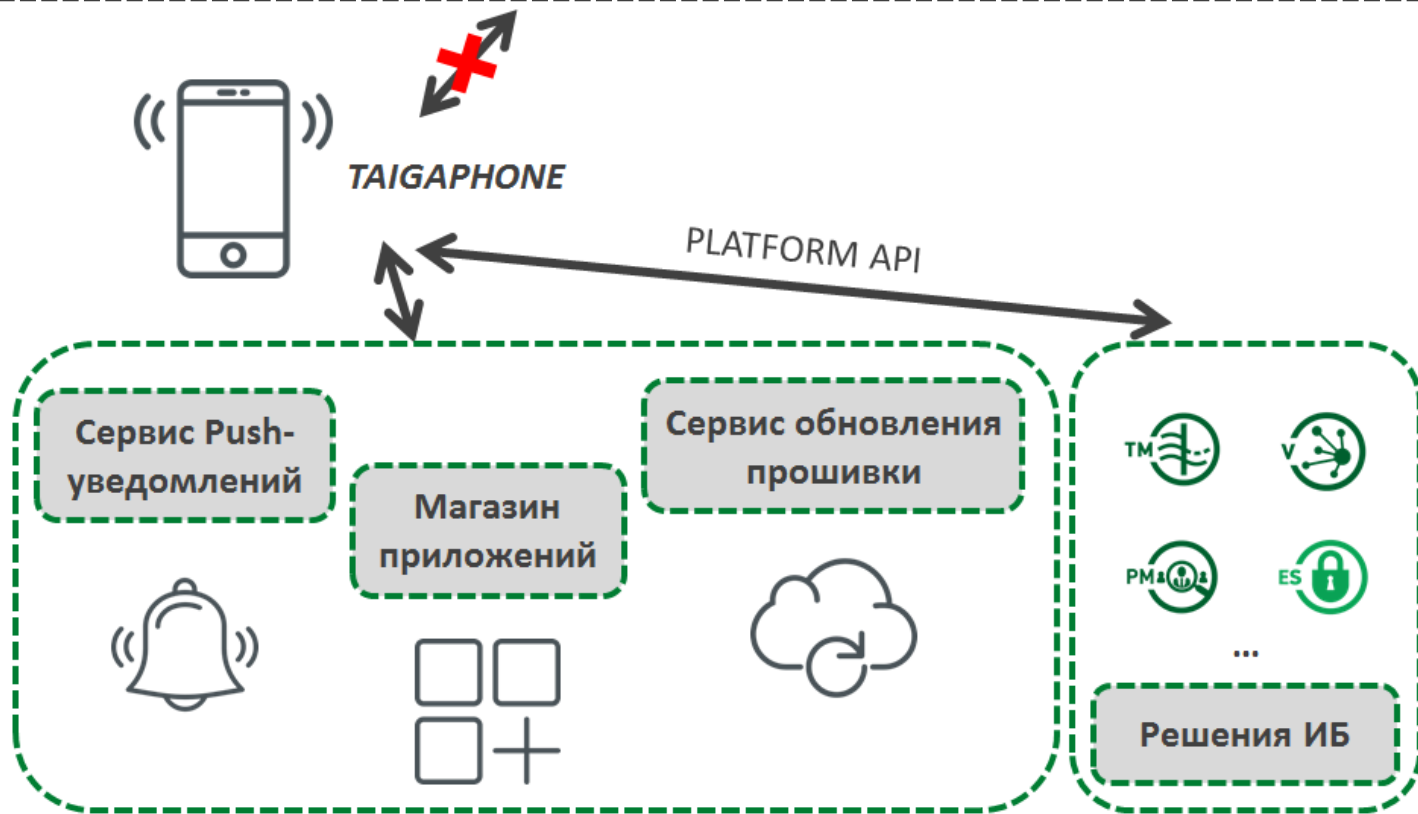
Предотвращение утечек конфиденциальных данных с устройства

InfoWatch Taigaphone – смартфон с доверенной прошивкой на базе Android, тесно интегрирующийся с InfoWatch Traffic Monitor

Схема работы



Зарубежные сервисы





- ✓ Сервер Push-уведомлений
- ✓ Магазин приложений
- ✓ Сервер обновления прошивки
- ✓ Export API



« Использование продукта InfoWatch в связке с программным обеспечением, необходимым для работы Правительства Северной Осетии позволит сотрудникам республиканских ведомств и учреждений удаленно работать с документами в юридически значимом и безопасном формате. »



INFOWATCH®

МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Спасибо за внимание!

Григорий Васильев

Grigoriy.Vasilev@infowatch.com

Моб. +7 (916) 169 65 07