Международный ТБ ФОРУМ Технологии Безопасности

WorksPad Sk Skolkovo

Снижение рисков использования мобильных устройств для доступа к корпоративной информации

Сергей Орлик

Генеральный директор «МобилитиЛаб»

2018

Мобильность: факты и тенденции

“К 2022 году 70% всех взаимодействий с корпоративными системами будет осуществляться с мобильных устройств.”

Gartner, Predicts: 2017 Mobile Apps and Their Development forecasting
https://www.enterprise-cio.com/news/2017/jan/04/why-2017-will-be-year-continued-evolution-enterprise-mobility/

“75% нарушений безопасности связанных с мобильными устройствами являются результатом неправильного использования и конфигурирования мобильных приложений, а не атак на мобильные устройства.”

Gartner, Mobile Security Threats and Trends
https://www.gartner.com/newsroom/id/2753017

Мобильность часто воспринимают и используют вместе с облачными сервисами.
“В 2017 году информация стала намного чаще утекать в результате как умышленных, так и случайных действий. Исследователи безопасности практически ежедневно стали сигнализировать о незащищенных облачных серверах.“

InfoWatch, Главные утечки 2017 года
https://www.infowatch.ru/analytics/digest/19546

Проблемы мобильности в корпоративной среде

Проблема 1: мобильные устройства – недоверенные

Мобильных устройств “не существует”
в корпоративных регламентах ИБ

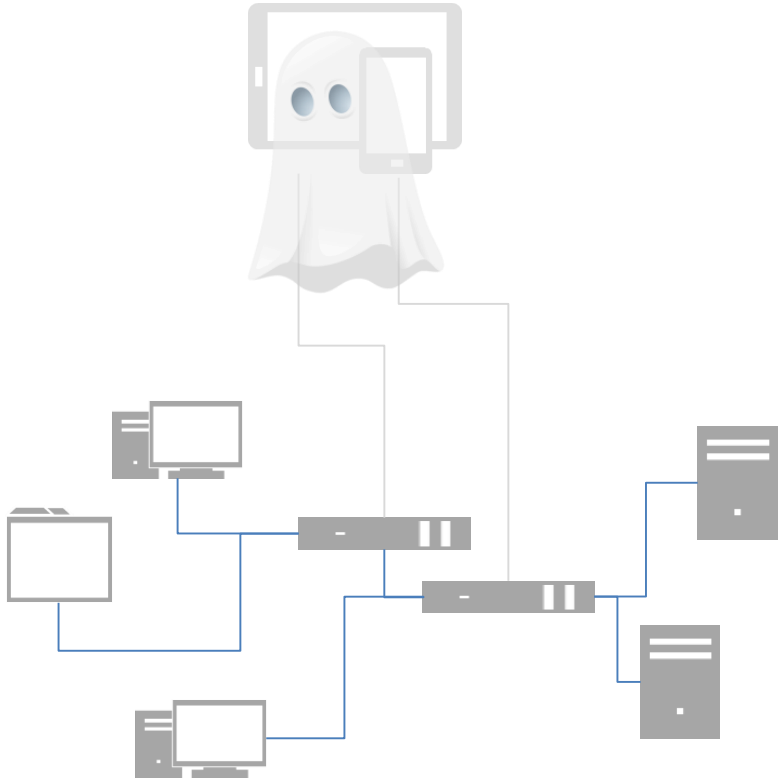
Мобильное устройство ≠ Ноутбук

Мобильные устройства = iOS & Android

О мобильных устройствах вспоминают
когда “ложится” корпоративный Wi-Fi

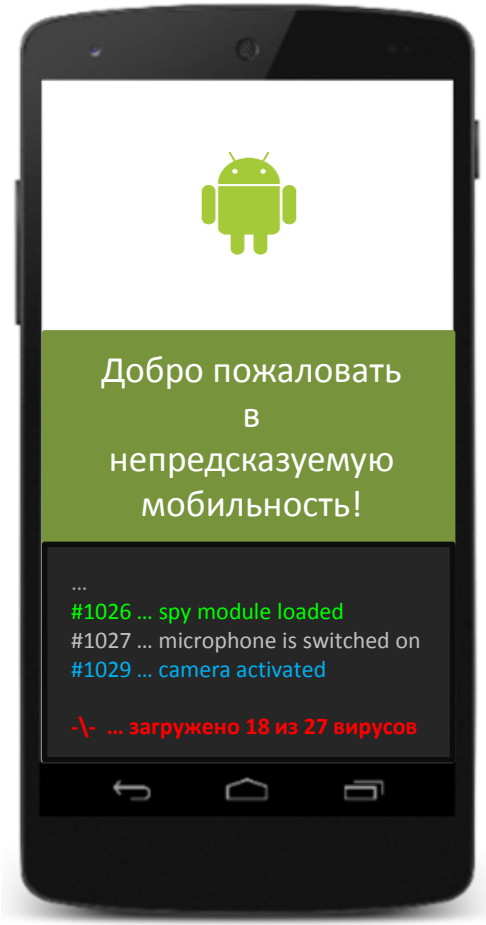
Если вспоминают о мобильных устройствах –
пытаются “защищать оконечное устройство”

“Мобильное устройство не является доверенным.
Их у нас нет”



Проблема 1: мобильные устройства – недоверенные

Отличия
iOS и Android
глазами ИБ

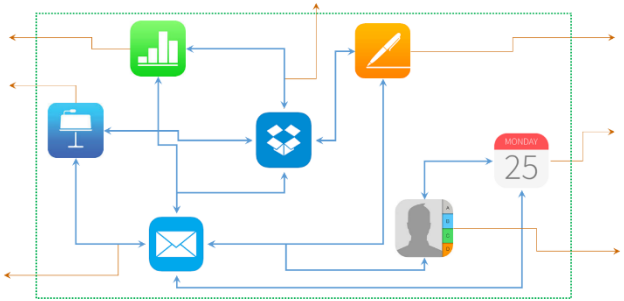


Проблема 2: мобильные приложения – недоверенные

Деловая информация в обычных потребительских приложения никак не контролируется и дублируется во множестве приложений

Современные мобильные платформы iOS и Android в основе своей ориентированы на обычных потребителей (consumers), мотивируя экосистему развиваться по принципу “одна функция – одно приложение”.

Приложения свободно обмениваются информацией (документами) через функцию ОС “открыть в”.



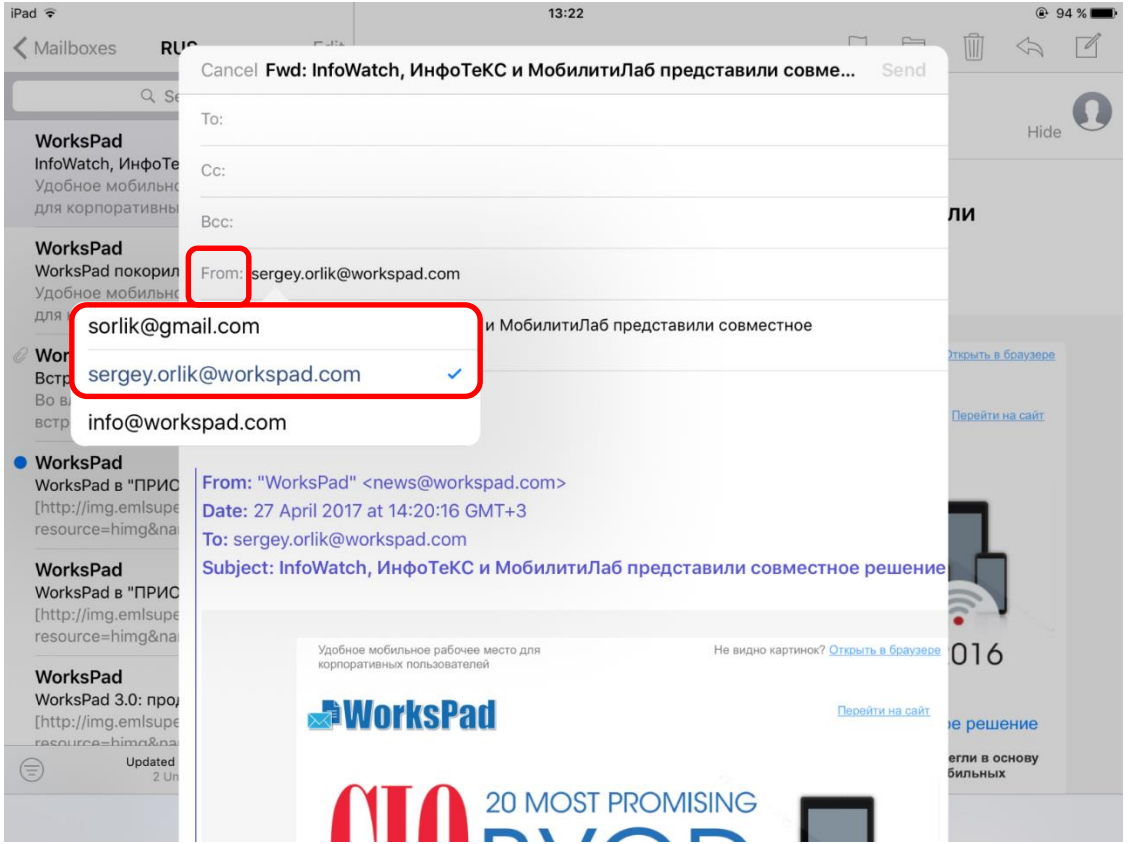
Информация неконтролируемо перемещается между приложениями

Проблема 2: мобильные приложения – недоверенные

Пользователи выводят данные из под ИБ-контроля меняя учетную запись почты несколькими касаниями в потребительских мобильных клиентах

Результаты:

- Утечки данных через взломанные личные учетные записи пользователей
- Инвестиции в традиционные системы защиты “не замечающие” мобильные устройства – обнуляются, создавая ложное ощущение защищенности у бизнеса



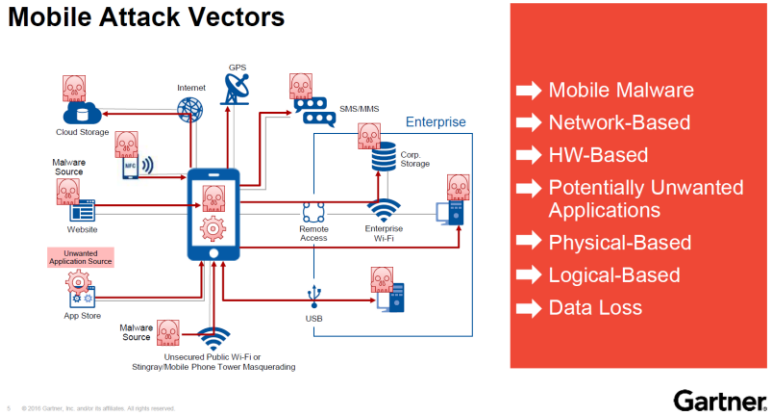
Проблема 3: мобильность данных - неконтролируема

Бесконтрольность корпоративных данных в потребительской среде
Легкость проникновения в периметр организации

Неконтролируемый обмен данными между приложениями через функцию “открыть в” (все мессенджеры, файло-обменники и почтовые клиенты умеют принимать любой контент) приводит к возникновению новых каналов и утечек и проникновения в корпоративную сеть

В ОС отсутствуют изолированные средства шифрования данных уровня приложения

Невозможно встроить в штатные ОС универсальные средства DLP аналогично тому как встраиваются VPN



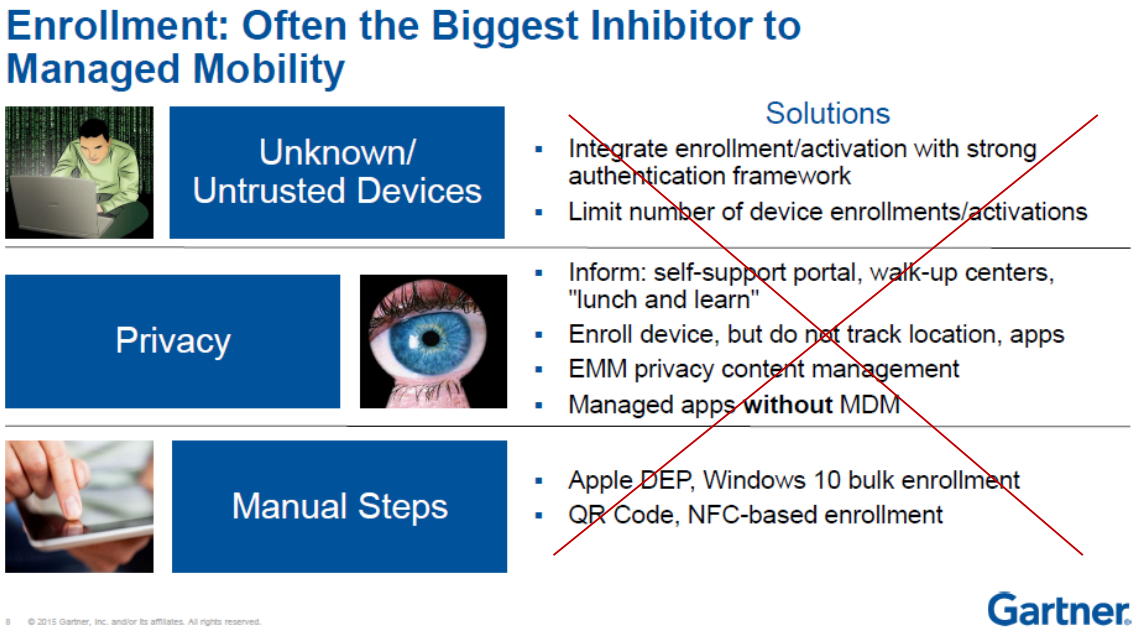
Источник: How to Build Your Next-Generation Mobile Security Strategy, Gartner

Проблема 4: личные устройства - безопасность и приватность

Пользователи против установки на личные устройства корпоративных средств управления мобильными устройствами – Mobile Device Management / Enterprise Mobility Management (MDM/EMM).

MDM/EMM привносит дополнительные затраты в инфраструктурный ИТ бюджет и требует доп. работы по развертыванию и контролю устройств, не решая проблему удобства доступа к информации.

Ограничения на личных устройствах не работают



Источник: Managing and Enabling Enterprise Mobility, Gartner

Решение

Решение ключевых проблемы мобильности

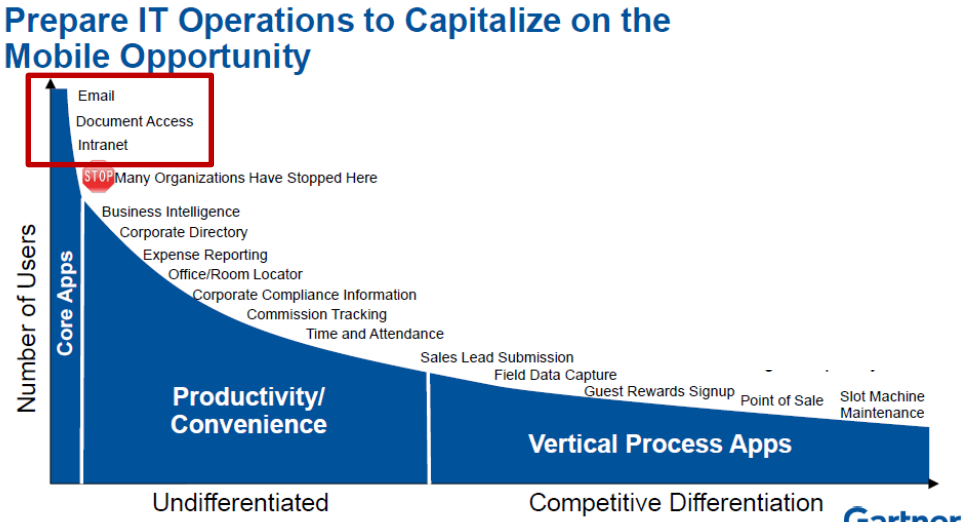
1. Доступ к корпоративной информации должен осуществляться из специализированных доверенных корпоративных приложений с запретом “открыть в” других приложениях

2. Разделение “корпоративного” от “личного” – защита данных в приложениях, а не устройствах, с возможным встраиванием DLP и дополнительного шифрования данных на уровне приложения

3. Поддержка модели BYOD без MDM/EMM без угрозы приватности и ущерба безопасности

С чего начинать безопасную мобильность

1. Безопасность мобильной работы необходимости начинать с наиболее часто используемых функций
   – почта, документы, интранет-сайты и web-клиенты к корп. системам
2. Специализированные приложения к корп. системам и боты к корпоративным системам только из доверенных корпоративных приложений
3. Специализированные корпоративные мессенджеры (есть вопросы к “облакам”)



Источник: Managing and Enabling Enterprise Mobility, Gartner

Базовые требования к защите данных в мобильных приложениях

1. Аутентификация в корпоративной службе каталогов
2. Контроль местоположения хранения информации на мобильном устройстве (НЕ /Documents на iOS, только системная память на Android)
3. Политики контроля выхода данных за пределы приложения и в приложение (запрет “открыть в” из приложения и в приложение)
4. Запрет резервного копирования данных приложения в облако (iCloud, Google) и на ПК (взлом бэкапа на порядки проще чем устройства, см. примеры Elcomsoft)
5. Идентификация факта взлома устройства (jailbreak, root) и запрет работы на таких устройствах, с возможным автоматическим стиранием данных приложения (wipe)
6. Политика маркировки экрана водяными знаками (запрет снятия копии экрана устройства средствами MDM обходится фотографированием экрана с другого устройства)
7. Контроль сетевых коммуникаций на отсутствие нерегламентированного взаимодействия с сервисами за периметром ИБ для встраиваемых библиотек на этапе разработки в SDLC (Secure Development LifeCycle, процесс разработки безопасных приложений)
8. Шифрование данных на устройстве при необходимости

Резидент ИТ кластера
«Сколково»

Обладатель Национальной премии
«Приоритет 2016»
в номинации «Программное обеспечение»

MobilityLab

Сергей Орлик, Генеральный директор
e-mail: sergey.orlik@workspad.com

e-mail: info@workspad.com
тел.: +7 (495) 974-7979

Рег. номер ПО WorksPad в Едином реестре российских программ для электронных вычислительных машин и баз данных: 4106

www.workspad.com **www.workspad.ru**