ФОРСАЙТ 2019 КОНФЕРЕНЦИЯ

Форсайт + НИИ СОКБ: защищенная мобильность

Олег Ассур, архитектор решения «SafePhone», компания «НИИ СОКБ»

Олег Бачурин, руководитель центра разработки мобильных решений компании «Форсайт»

ЗАЧЕМ НУЖЕН EMM?

EMM = **Enterprise Mobility Management**, управление корпоративной мобильностью

MDM

Mobile Device Management, управление мобильными устройствами

- Вести учёт мобильных устройств – какие устройства кому выданы
- Контролировать пользователей мобильных устройств:
  - Знать где находились мобильные устройства
  - Знать с кем общались пользователи мобильных устройств
- Обеспечить защищённость мобильных устройств:
  - Требовать, чтобы пароли доступа к устройствам были достаточно сложными для подбора и регулярно менялись
  - Препятствовать утечке данных с помощью политик безопасности и ограничению доступа к устройстве при утере / краже
- Поддерживать разные сценарии использования устройств:
  - Очень корпоративные устройства (COBO)
  - Корпоративные устройства в личном пользовании (COPE, CYOD)
  - Личные устройства (BYOD)
- Удобно управлять устройствами:
  - Регистрировать устройства быстро и просто
  - IT администраторы должны управлять тысячами устройств, тратя на это не больше нескольких часов в день

MAM

Mobile Application Management, управление мобильными приложениями

- Устанавливать приложения, нужные для работы
- Разделять корпоративное и личное:
  - Личное не трогать
  - Контейнер для корпоративных приложений с шифрованием данных, внутрь данные не пускать, наружу не выпускать
- Контролировать доступ к приложениям:
  - Удалить или заблокировать нежелательные приложения
  - Ограничить доступ только к одному приложению

MCM

Mobile Content Management, управление мобильным контентом

- Предоставить защищённый удалённый доступ к корпоративному контенту:
  - Электронной почте
  - Веб-порталам
  - Файлам
- Обеспечить удобную и защищённую связь между сотрудниками

РЕШЕНИЕ «SAFEPHONE»

Сценарии установки

- Сервер можно:
  - Установить локально (on-premise)
  - Не устанавливать и получить доступ из «облака» (SaaS)
- Клиент может установить:
  - Администратор
  - Пользователь
  - Само устройство, если его сделал Samsung

Дистанционное управление

- Если устройство потеряли или украли, его можно:
  - заблокировать и найти по GPS;
  - сбросить к заводским настройкам или удалить с него корпоративные данные
- Если пользователь забыл пароль, можно его сбросить и потребовать установить новый

Сбор информации

- Соберём и запишем данные о мобильных устройствах:
  - Местоположение
  - Звонки
  - SMS
- Если не нужно, не будем записывать

Управление политиками

- Потребуем какими должны быть пароли и как часто их нужно менять
- Не дадим пользователю возможности «слить» данные:
  - заблокируем интерфейсы записи и передачи данных
  - не дадим доступа ко встроенным приложениям и функциям
  - запретим только то, что нужно
- Добавим на устройство Exchange аккаунт, пароль пользователь укажет сам, мы пароли не храним
- Настроим доступ к корпоративному Wi-Fi
- Установим настройки доступа в сеть сотового оператора, если он этого не сделал
- Обеспечим правильное время на устройствах, даже если сотовый оператор не предоставляет такой услуги
- Кастомизируем устройства в вашем стиле: установим обои рабочего стола, анимацию при загрузке и др.
- Распространим актуальные политики автоматически
- Предложим сделать разные политики для:
  - разных групп пользователей (руководство, офисные и удалённые сотрудники)
  - корпоративных и личных устройств
  - разного местоположения устройств

РЕШЕНИЕ «SAFEPHONE»

Управление приложениями

- Автоматически установим нужные корпоративные приложения и приложения из публичных магазинов
- Дадим пользователям возможность самостоятельно установить приложения из корпоративного «магазина»
- Настроим режим «киоска», если пользователям нужен доступ только к одному приложению
- Запретим приложения по принципу «чёрного» или «белого» списка, если они небезопасны или мешают работе
- Распространим приложениям настройки, чтобы пользователю не нужно было их указывать
- Соберём логи приложений, использующих SafePhone SDK, и отдадим их в SIEM или разработчикам приложений

Настройка доступа к почте

- Почта нужна всем. Мы предлагаем:
  - Настроить встроенные почтовые клиенты iOS и Samsung – они есть на устройствах «из коробки»
  - Настроить приложения Gmail и Outlook, если вы ими пользуетесь
  - Собственный защищённый почтовый клиент для iOS
- Чтобы не создавать для каждого пользователя собственные настройки, укажите «шаблоны» вместо домена, логина и ящика электронной почты, а мы заполним их данными пользователя автоматически

Контейнеры

- Настроим контейнер Knox на устройствах Samsung
- Для других устройств защитим корпоративные данные с помощью доработки приложений. Доработка может быть:
  - Добровольной, когда разработчик сам встраивает SafePhone SDK в своё приложение
  - Принудительной, когда SafePhone SDK в приложение добавляет администратор с помощью SafePhone Wrapper
- Доработка приложений защитит ваши данные:
  - Данные приложений будут зашифрованы
  - Пользователь не сможет вынести данные из приложения без вашего разрешения

Администрирование

- Предложим настроить разный интерфейс для администраторов IT и офицеров ИБ и любых других ролей
- Загрузим данные пользователей из каталога MS AD
- Соберём все логи в единое хранилище, чтобы вы могли передать их в SIEM или нашей техподдержке, если потребуется
- Покажем администраторам дашборды с показателями «здоровья» системы сейчас и за период, они это любят
- Сообщим администраторам, если серверы перестанут работать как надо

РЕШЕНИЕ «SAFEPHONE»

Прикладные сервисы

- На iOS нет встроенных контейнеров, поэтому для защищённого удаленного доступа нужны специальные приложения. У нас есть:
  - Почтовый клиент iOS для работы с Exchange
  - Веб-браузер iOS для просмотра веб-страниц в защищённом режиме
- Dropbox – это удобно, но небезопасно, наш корпоративный аналог безопасен и может дать пользователям доступ к вашим файловым хранилищам
- WhatsApp не годится для корпоративного общения, потому что ваши данные не у вас. Мы предлагаем защитить ваше общение:
  - VoIP связь с возможностью вызова абонентов корпоративной АТС
  - Обмен текстовыми и мультимедиа сообщениями
  - Общение в режиме рации (push-to-talk)
  - Персональные «белые» и «чёрные» списки абонентов – недовольный сотрудник не побеспокоит председателя правления

Почему SafePhone?

- Полностью разработан в России:
  - Поможем, если импортозамещение и санкции для вас актуальны
  - Интерфейс и документация на русском языке. Вам не придётся переводить документацию, чтобы написать внутренние документы
- Техническая поддержка из России:
  - Не нужно писать в международную поддержку на английском и ждать пока они поймут в чём проблема
  - Можем приехать, чтобы помочь решить проблему
- Есть сертификат ФСТЭК России на актуальную версию
- Собственный коллектив разработчиков, который может выпустить обновление для решения ваших задач
- Гибкая «дорожная карта» с учётом потребностей Заказчиков
- Лидер на рынке российских EMM, конкурирует с мировыми лидерами
- Успешные крупные внедрения в России
- Знаем и умеем внедрять в России крупные EMM проекты, поэтому можем спроектировать и внедрить мобилизацию «под ключ»

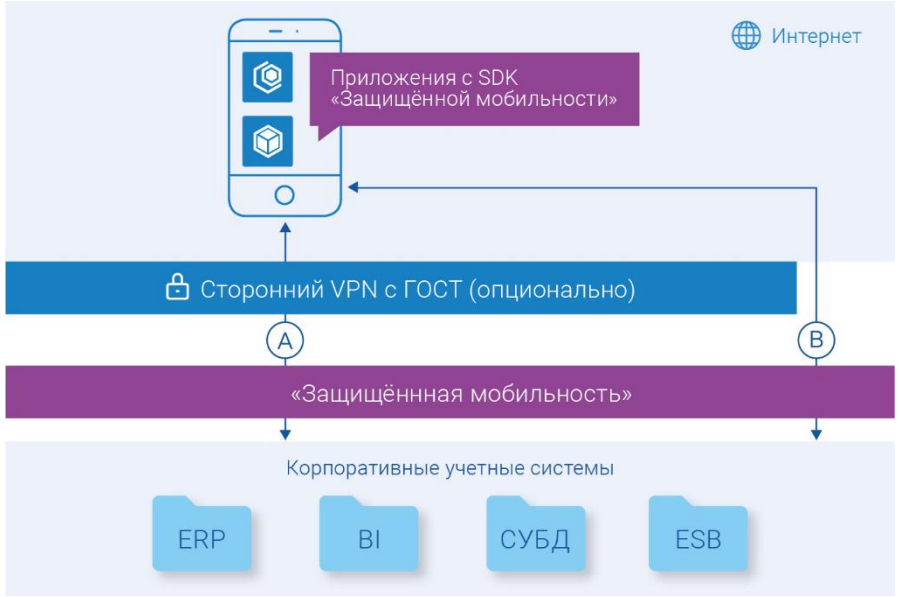
РЕШЕНИЕ «ЗАЩИЩЕННАЯ МОБИЛЬНОСТЬ»

Комплексное решение, которое включает перечень готовых защищенных приложений, позволяет разрабатывать мобильные приложения для бизнеса любой сложности в кратчайшие сроки и обеспечивает информационную безопасность мобильной экосистемы предприятия

Защищённая мобильность	Форсайт. Мобильная платформа	Платформа SafePhone

Преимущества решения

- Сертифицированное средство защиты информации
- Готовые к использованию защищенные мобильные приложения
- Централизованное безопасное управление мобильными устройствами и приложениями
- Готовая методология по разработке корпоративных мобильных бизнес-приложений
- Готовые коннекторы к учётным системам, системам отчётности и СУБД
- Интеллектуальный обмен данными между мобильным приложением и решением «Защищённая мобильность» (сервер «Форсайт. Мобильной платформа»), включая скоростную, потоковую передачу больших объёмов данных
- Централизованное ведение пользователей



A Сертифицированное средство криптографической защиты информации для соблюдения строгих требований информационной безопасности

B Несертифицированное средство криптографической защиты информации, применяется для проектов, не требующих соблюдения строгих требований информационной безопасности, позволяет снизить материальные затраты. Решение удовлетворяет требования продуктов: «Технический обход и ремонт оборудования (ТОРО)», «Приемка и размещение товара на складе», «Инвентаризация» и т.п.