www.pwc.com

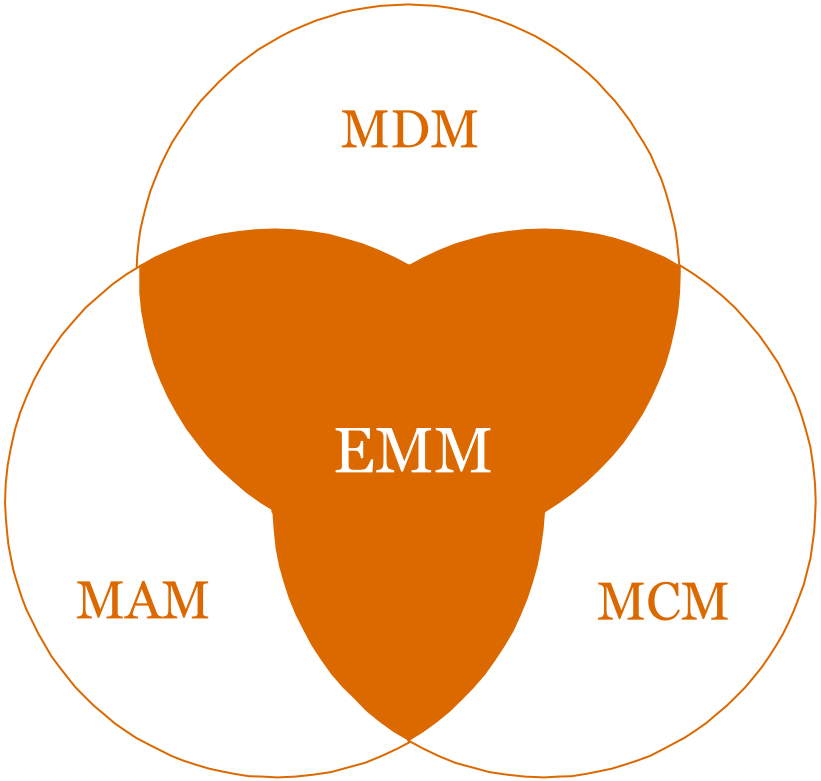
Выбор MDM решения

Вопросы эффективности и безопасности

Ноябрь 2014

pwc

Различные M



MDM – Mobile Device Management – фокус на управлении устройством

MAM – Mobile Application Management – фокус на управлении приложениями, безопасном подключении приложений к инфраструктуре

MCM – Mobile Content Management – фокус на безопасном хранении документов через одно приложение-контейнер

EMM – Enterprise Mobility Management – комплексное решение

Первые вопросы при выборе

- Кому принадлежат устройства – BYOD/COPE?
- Куда нужен доступ с устройств?
- Будут ли подключаться поставщики/контрагенты/клиенты?
- Какие платформы необходимо поддерживать?
- Где расположена основная инфраструктура – внутри/в облаке?
- На каких технологиях/решениях основана инфраструктура?

Внутри или в облаке?

- У большинства решений есть обе версии
- Облачные решения есть и у операторов связи
- Облачные решения делают MDM доступной для малого и среднего бизнеса
- Выбор зависит от ресурсов, текущей инфраструктуры, набора корпоративных приложений

Управление устройствами

- Набор политик достаточно стандартный, основан на API OS
- Есть различия в интеграции с AD, деталях управления
- Есть различия в поддерживаемых платформах

Управление приложениями

- App wrapping – политика доступа, ограничение действий через API, ограничение сетевого доступа и пр.
- Корпоративные каталоги приложений
- Белые / Чёрные списки приложений, репутационные сервисы
- Проверка приложений на вредоносный код

Контейнеризация

- В том или ином виде есть у любого решения
- VPN на уровне приложения
- Шифруются коммуникации между приложениями
- Безопасный браузинг, DNS запросы

Выбор производителя

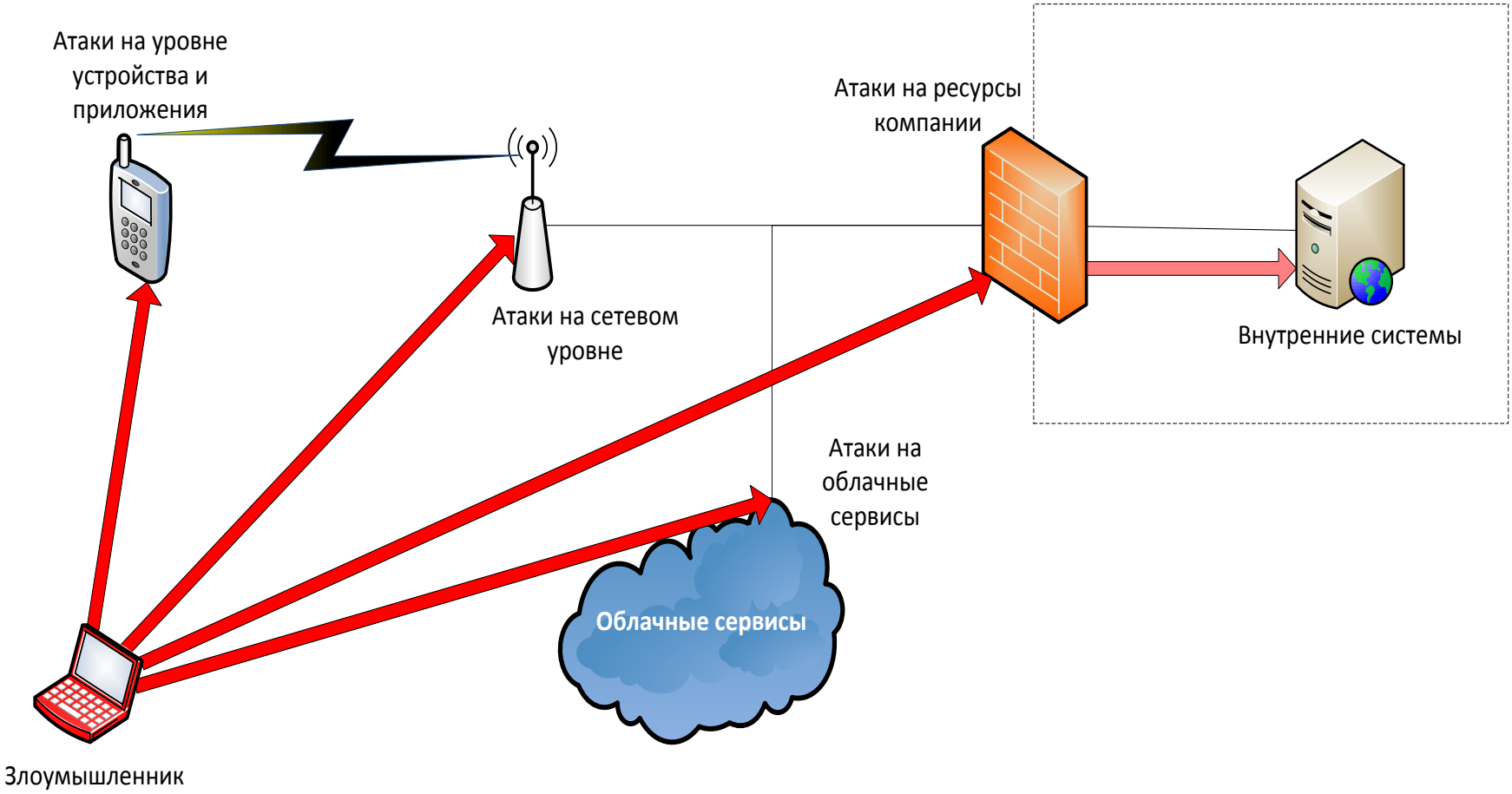
- Выбирайте решение близкое вашей инфраструктуре
- Работайте с интегратором, предлагающим много продуктов
- Проведите пилотное внедрение

Но не всё работает так, как написано
Нужно проверять…

Документы

- NIST 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- OWASP Mobile Security Project
- PCI Mobile Payment Acceptance Security Guidelines
- Evaluation of mobile device management tools and analysing integration models for mobility enterprise, 2013
- Security Evaluation of MobileDevice Management Solutions, 2014
- Многочисленные рекомендации производителей

Векторы атак

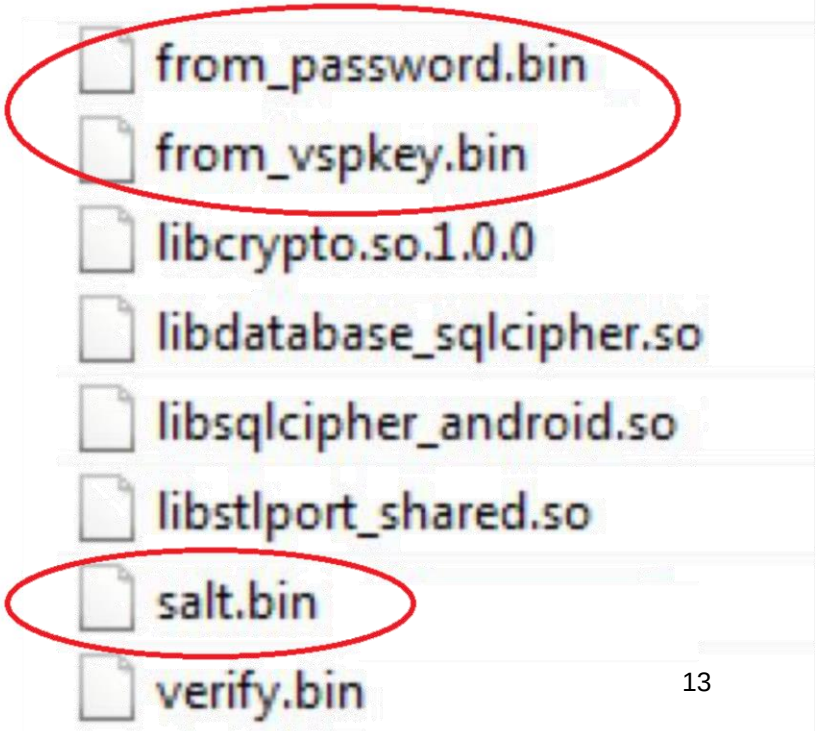


Сценарии

- Украденное устройство
- Любопытный пользователь
- Устройство в недоверенной сети
- Уволенный (уволившийся) сотрудник
- Заражённое устройство

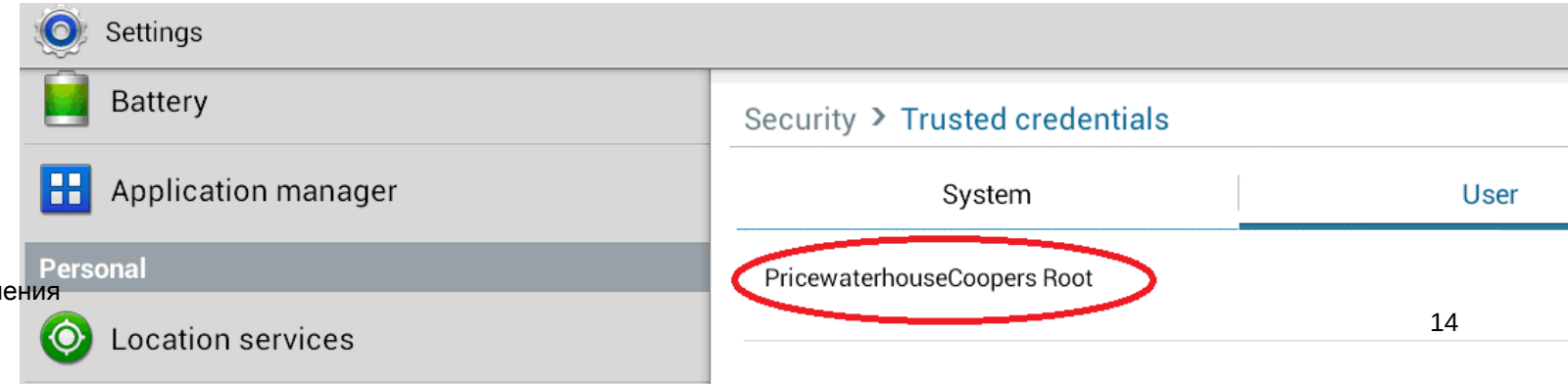
Шифрование данных

- Не забудьте про карты памяти
- Проверьте как обрабатываются зашифрованные почтовые сообщения
- Как хранятся почтовые вложения
- Где и как хранятся пароли и хэши



Что остаётся после отключения устройства от MDM

- Иногда, если пользователь удалил MDM агент вручную остаётся всё
- На Android остаются сертификаты x.509
- Данные вне контролируемых приложений
- Данные «в облаках» и синхронизированные с другими устройствами

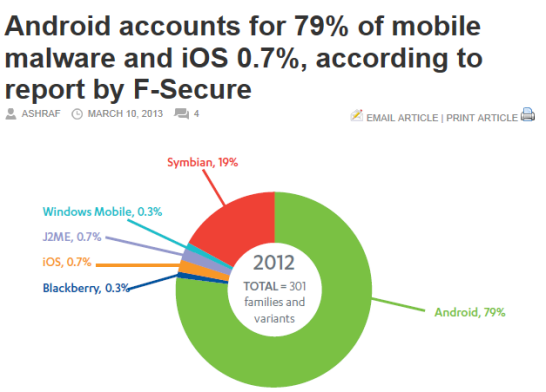


Проверка эффективности политик

- Запрет jailbroken/rooted устройств
- Действия MDM со взломанным устройством, в т.ч. при недоступности MDM сервера
- Возможность подключиться к внутренним системам (например, почте) напрямую, минуя запреты MDM системы
- Возможность подделать статус устройства
- Соответствие реальной политики заявленной

```
System.out          # before wipe: 0
System.out          Time before wipe: 0
System.out          Password expiration in: 0
System.out          Password history length: 1
System.out          Minimum password length: 9
System.out          Minimum lowercase: 0
System.out          Minimum nonletter: 0
System.out          Minimum numeric: 1
System.out          Minimum symbol: 1
```

Malware…



- Запрещена ли установка приложений из недоверенных источников
- Какие механизмы защиты от вирусов используются
- Не позволяет ли само приложение MDM манипулировать собой сторонним процессам

Контейнеры…

- Проверьте, не оказываются ли данные «снаружи»:
  - При подключении к корпоративным ресурсам через браузер
  - Просто через буфер обмена …
  - Временные файлы, записи в журнале

Сам портал MDM

- Обход авторизации при регистрации устройства
- Перехват конфиденциальных данных
- Уязвимости самого web-приложения

Вопросы?

Владимир Наймарк

T: +7 (495) 223-5047
M: +7-906-789-61-10
E: vladimir.naimark@ru.pwc.com