КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как обеспечить защиту корпоративной информации на мобильных устройствах:

обзор возможностей управления различных мобильных платформ.

Кирилл Богданов
Microsoft

Кирилл Богданов

```
PS C:\> Get-Speaker $kirbogd

Имя:    Кирилл Богданов

Должность:    Эксперт по решениям Microsoft в ИБ

Описание:    6 лет борьбы за безопасные облака в крупных заказчиках

Предыдущий опыт
     :  Системный архитектор
     :  Системный инженер
     :  "Полевой" инженер

@Twitter:    @Kirbogd

@Telegram:    https://t.me/kirbogdITS
```

#CODEIB

Содержание:

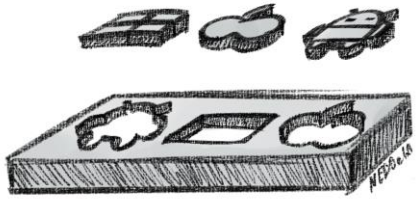
- Управление мобильными устройствами – не простая задача
- Режимы управления:
  - **iOS**
  - **Mac OS X**
  - **Android**
  - **Windows**

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В ЧЕМ ПРОБЛЕМА?

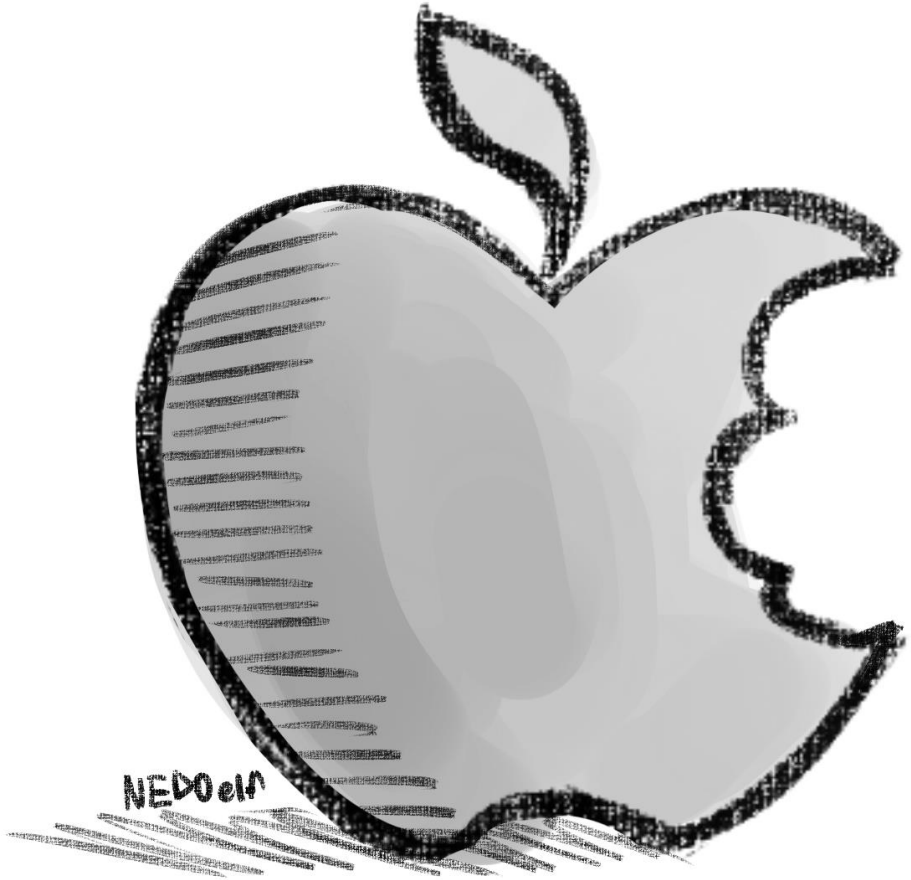
ЛИЧНОЕ УСТРОЙСТВО = ЛИЧНОЕ УСТРОЙСТВО
И производители за этим следят

ЦЕЛОСТНОСТЬ СИСТЕМЫ БЕЗОПАСНОСТИ
Нельзя просто взять и сделать jailbrake



РАЗНЫЕ ПЛАТФОРМЫ = РАЗНЫЕ ПРАВИЛА
Каждая из платформ (а часто и версий) имеет свой API и ограничения

iOS



BYOD Личные устройства

1 Все приложения изолированы и ограничены

2 Последнее слово за пользователем

3 Поддерживаются профили доступа

4 Есть разграничение контекста

5 Можно «перехватить» приложение

6 Очистка устройства возможна

USER ENROLLMENT

ПОЯВЛЯЕТСЯ В iOS 13

ИЗОЛЯЦИЯ КОРПОРАТИВНЫХ ДАННЫХ

МНОЖЕСТВО ПАРАМЕТРОВ
- Приложения
- VPN
- Профили настроек

ТРЕБУЕТ MANAGED APPLE ID И APPLE BUSINESS MANAGER

SUPERVISED

1

УСТРОЙСТВО ПРИНАДЛЕЖИТ ОРГАНИЗАЦИИ

2

ДВА ВАРИАНТА ВКЛЮЧЕНИЯ РЕЖИМА

- APPLE CONFIGURATOR
- DEVICE ENROLLMENT PROGRAM

3

ДВА РЕЖИМА РАБОТЫ

- USER AFFININITY
- NO USER

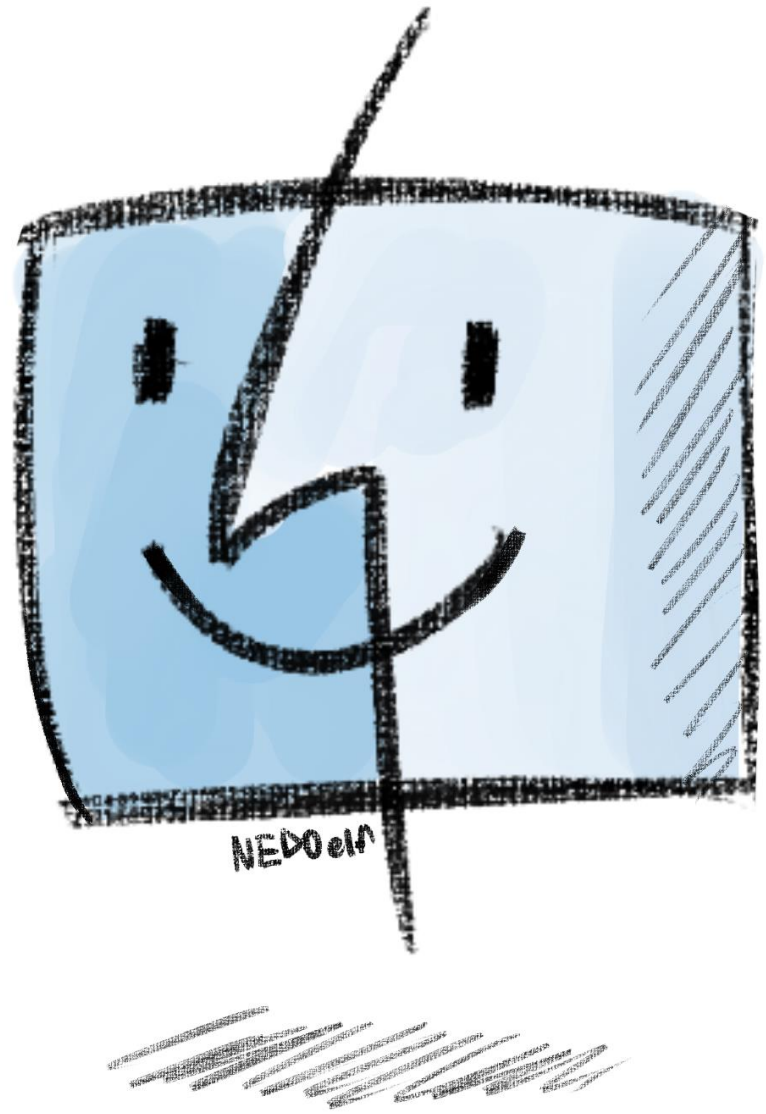
4

МАКСИМАЛЬНЫЕ ВОЗМОЖНОСТИ

- Ограничения
- Киоск
- Профили

КИОСК БЕЗ ПОЛЬЗОВАТЕЛЯ ТРЕБУЕТ VOLUME PURCHASE PROGRAM

Mac OS X



БАЗОВОЕ УПРАВЛЕНИЕ БЕЗ ОСОБЫХ СЮРПРИЗОВ

1

РАЗДЕЛЯЕТ УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ И УСТРОЙСТВОМ

2

АВТОМАТИЧЕСКАЯ РЕГИСТРАЦИЯ С DEP

3

НАСТРОЙКА СРЕДСТВ БЕЗОПАСНОСТИ

- Пароль
- Шифрование диска
- Фаервол
- Сброс

4

ПРОФИЛИ ПОДКЛЮЧЕНИЙ

- Сертификаты
- VPN
- Wi-Fi

5

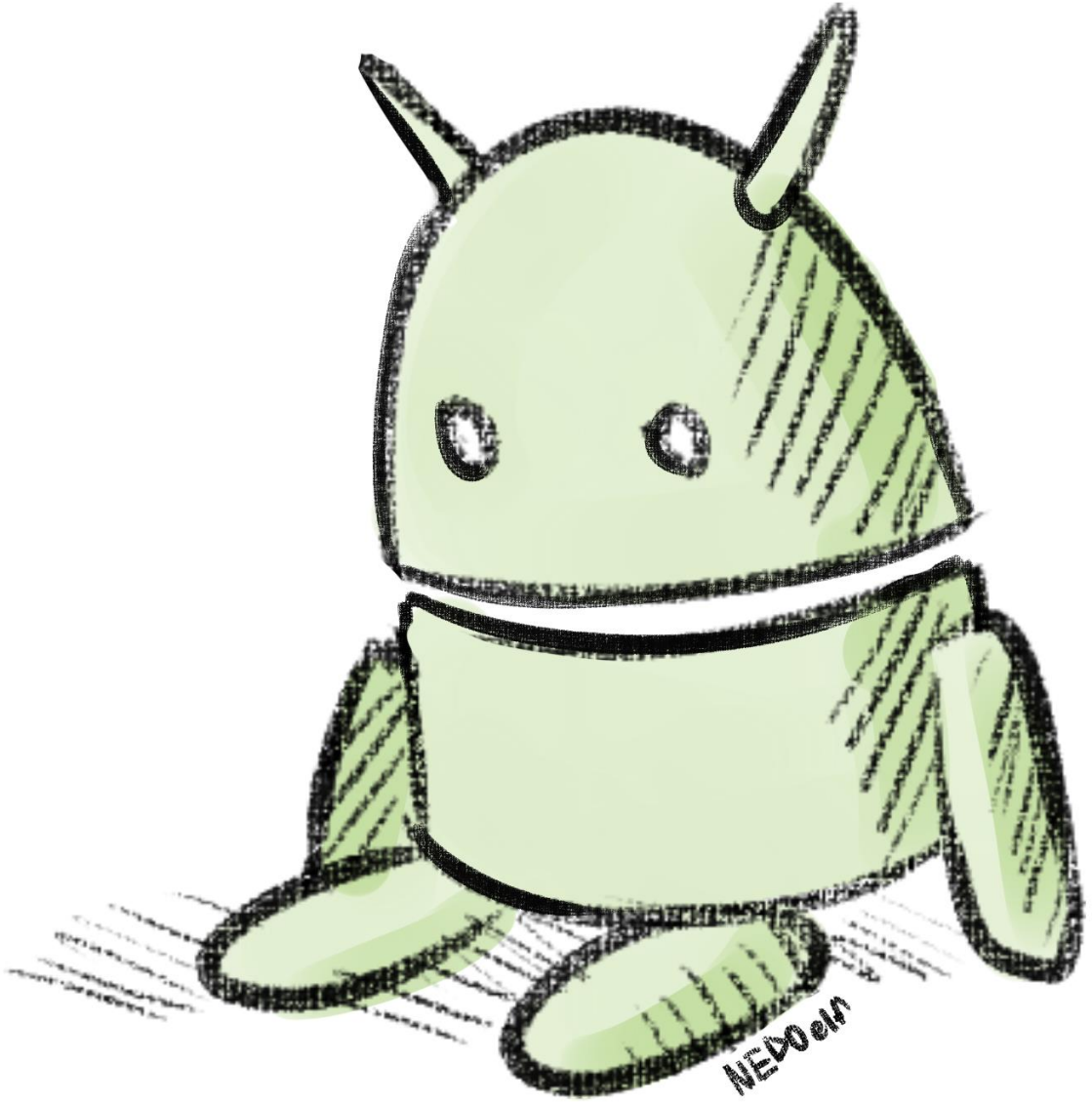
УСТАНОВКА ПРИЛОЖЕНИЙ

6

ОБНОВЛЕНИЕ ОС

Требует DEP

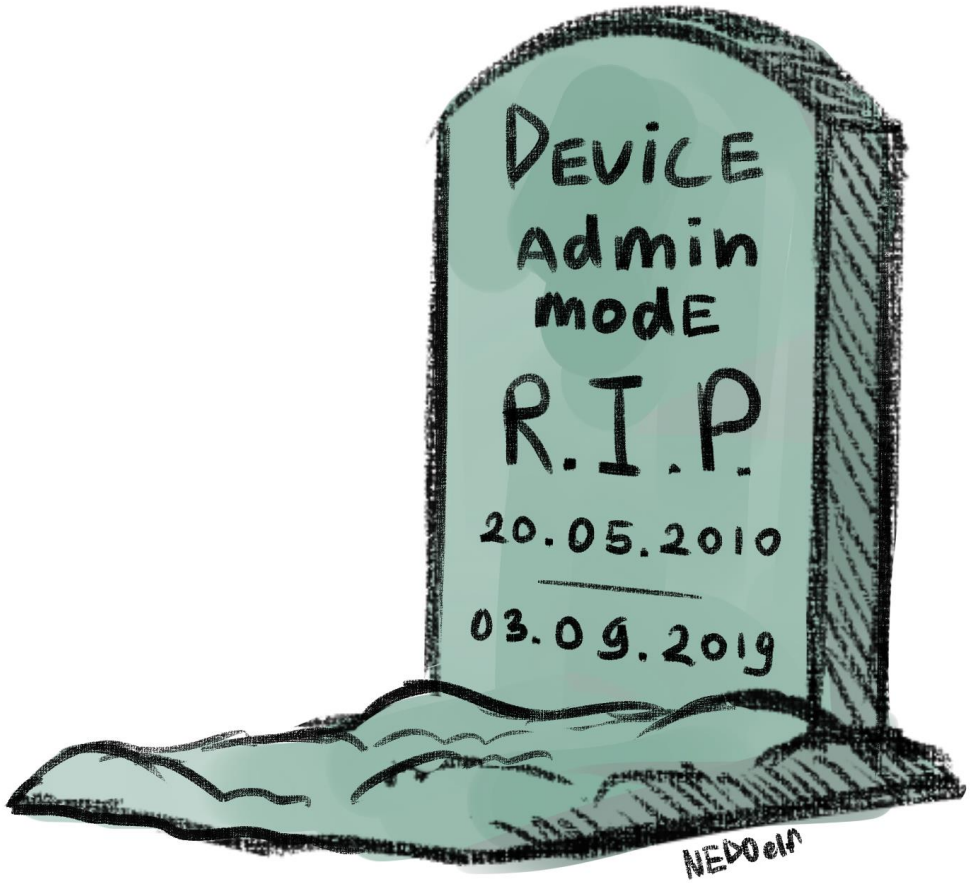
Android



Device Admin Mode

ОГРАНИЧЕННЫЙ API

- ПАРАМЕТРЫ ПАРОЛЯ (тип, длина, история)
- АВТОБЛОКИРОВКА
- ШИФРОВАНИЕ ДИСКА
- ОТКЛЮЧЕНИЕ КАМЕРЫ
- УДАЛЕННАЯ БЛОКИРОВКА
- УСТАНОВКА ПРИЛОЖЕНИЙ
- СЕРТИФИКАТЫ
- VPN



ANDROID ENTERPRISE

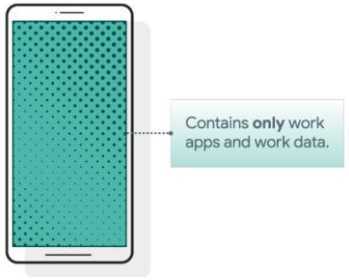
COMPANY OWNED

ANDROID 5.1
(НА САМОМ ДЕЛЕ – 6.0)

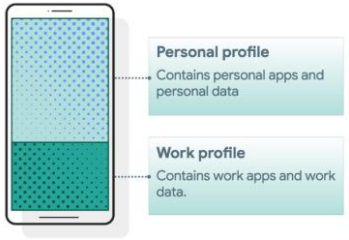
ИЗОЛИРОВАННЫЕ РАЗДЕЛЫ В ОС

РАЗЛИЧНЫЕ РЕЖИМЫ
- Work Profile
- Device Owner

COMPANY OWNED DEDICATED DEVICE (COSU)
- Моноцелевые киоски
- Параметры ограничения среды
- Wi-FI
- Установка приложений



COMPANY OWNED DEVICE
- Полностью контролируемая среда
- Установка приложений
- Настройка профилей



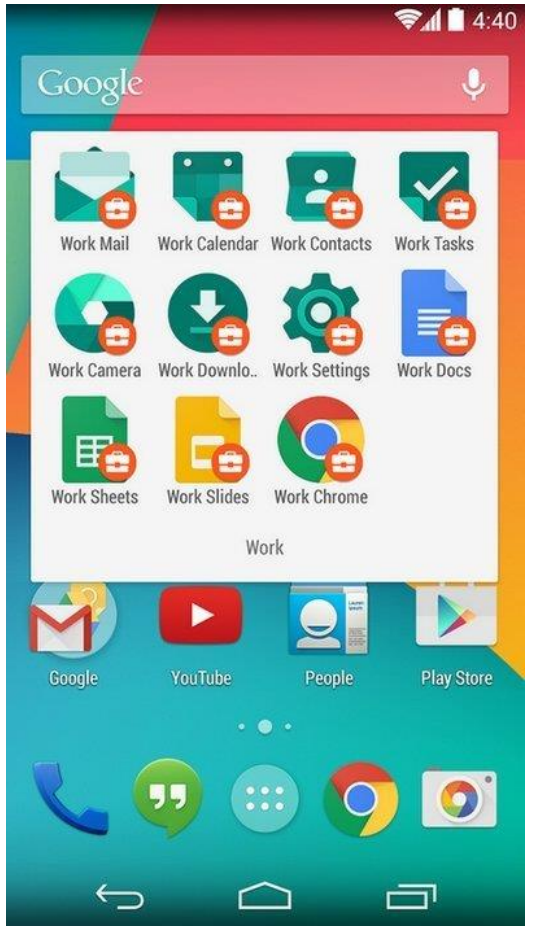
COMPANY OWNED DEVICE WITH PERSONAL PROFILE
- Имеется личный профиль
- Рабочая среда дополнительно изолирована от личной

ANDROID ENTERPRISE

WORK PROFILE

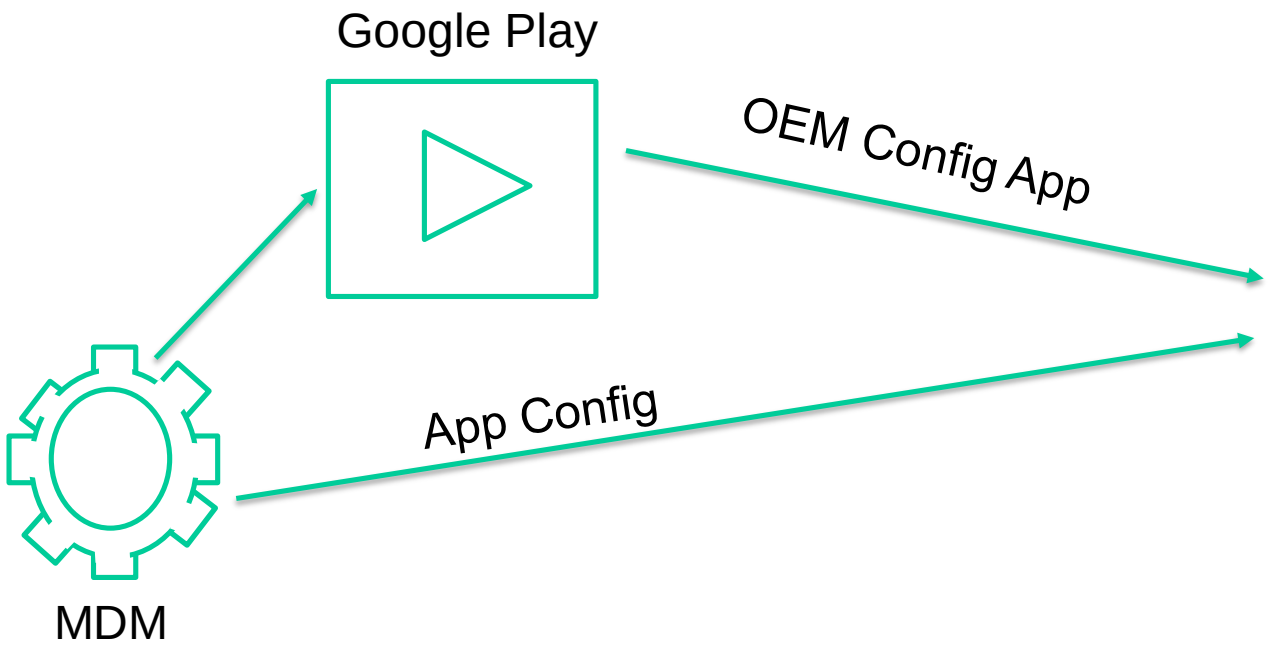
Рабочая зона на персональном устройстве

- Приложения через Play for Work
- VPN
- Сертификаты
- ПИН рабочей области
- Запрет передачи данных
- Персональные данные и файлы недоступны администратору



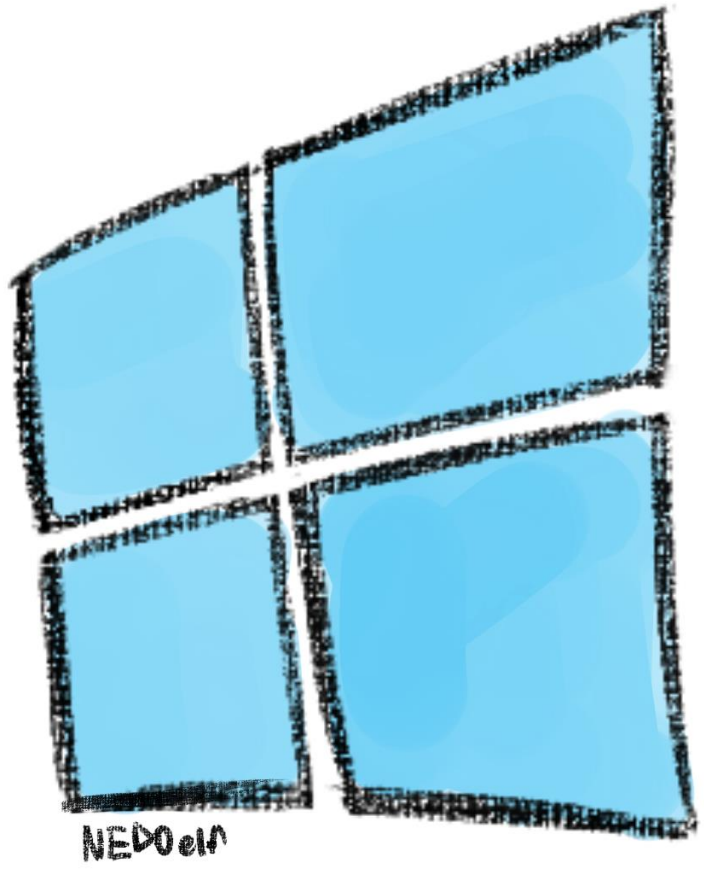
ANDROID ENTERPRISE

OEM Config



РАСШИРЕНИЯ API ОТДЕЛЬНЫХ ПРОИЗВОДИТЕЛЕЙ

Windows



Modern Desktop Management

1

ОСНОВНОЙ СПОСОБ УПРАВЛЕНИЯ ОС

2

ПОДДЕРЖКА AUTOENROLLMENT

Windows Autopilot

3

ПОЛНОЕ УПРАВЛЕНИ ОС

Обновления

Профили подключения

4

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

Firewall

Defender Antivirus

Defender ATP

BitLocker

App Guard

Security Baselines

5

УСТАНОВКА ПО И СКРИПТЫ

Windows Store 4 Business

APPX

MSIX

MSI

EXE

PowerShell

6

КИОСКИ И СПЕЦ УСТРОЙСТВА

Режим киоска

Средства Windows Embedded Tools

MAM w/o enrollment

НЕЗАКОНЧЕННАЯ ПОПЫТКА СДЕЛАТЬ BYOD НА WINDOWS

НАСТРОЙКА WINDOWS INFORMATION PROTECTION
Разделение файлов и контекста на рабочий / личный
Управление движением корпоративной информации

ИСПОЛЬЗУЕТ МЕХАНИЗМ AZURE AD JOIN
в рамках добавления учетной записи
можно применить политику к устройству

ТРЕБУЕТ WINDOWS 10 PRO ИЛИ ENTERPRISE
И средства изоляции WINDOWS 10 HOME пока отсутствуют

ВЫВОДЫ

КАК ОБЕСПЕЧИТЬ ЗАЩИТУ КОРПОРАТИВНОЙ ИНФОРМАЦИИ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

1

ПРАВИЛЬНО ВЫБИРАЙТЕ ПЛАТФОРМУ И РЕЖИМ

Ваши требования могут быть реализованы не на всех платформах

2

ПРИ ВЫБОРЕ ПЛАТФОРМЫ УПРАВЛЕНИЯ УЧИТЫВАЙТЕ РЕЖИМЫ

Плоский RFI не даст объективной картины

3

ЧАСТЬ ЗАЯВЛЕННЫХ ВОЗМОЖНОСТЕЙ НЕ БУДУТ ДОСТУПНЫ

Учитывайте в стратегии

4

MDM в BYOD – ЛИШЬ ЧАСТЬ РЕШЕНИЯ

Контроль устройства не дает гарантии защиты информации (нужен контроль приложений/контекста)

Полезные ссылки

https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference
https://docs.microsoft.com/en-us/windows/client-management/manage-windows-10-in-your-organization-modern-management
https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf
https://developer.apple.com/business/documentation/MDM-Protocol-Reference.pdf
http://www.androiddocs.com/guide/topics/admin/device-admin.html
https://support.google.com/googleplay/work/answer/6257696
https://developers.google.com/android/work/overview#company-owned-devices-for-knowledge-workers

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

Кирилл Богданов

https://twitter.com/Kirbogd
https://t.me/KirbogdITS


КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ