**Название**: «Как обеспечить защиту корпоративной информации на мобильных устройствах: обзор возможностей управления различных мобильных платформ.»

О докладчике: Кирилл Богданов – эксперт по решениям в области ИБ корпорации Microsoft. Более пяти лет помогает крупным корпоративным заказчикам Microsoft в России обеспечивать безопасное использование облачных сервисов и сред, а также мобильных устройств. В качестве докладчика выступал на проводимых Microsoft (“Microsoft Платформа Цифрового Бизнеса”, “На острие атаки: практическая безопасность”, “CIO Summit”, ”IT Conference: Облако в России”, “IT Pro Community Day”, Retail Innovation Day: угадывая будущее) и внешних конференциях («Positive Hack Days 2019», «Infosecurity Russia 2018: Эволюция облаков и ЦОДов в эпоху цифровой трансформации», «Инфофорум 2017», и др.).

**Тема**: Мобильные устройства и платформы прочно обосновались в нашей повседневной жизни и так же уверенно входят в жизнь корпоративную. Специализированные устройства, элементы автоматизации бизнес-процессов, мобильные рабочие места и, конечно, персональные устройства сотрудников. Но мобильные устройства — это не только отдельный форм-фактор. Это еще и собственные ОС, со своими правилами и ограничениями, которые могут очень сильно расходиться с ожиданиями, основанными на традиционных средах. В рамках доклада мы рассмотрим на примерах iOS, Mac OS, Android и Windows, какие методы и режимы управления поддерживаются, и что каждый из режимов позволяет сделать с точки зрения конфигурирования и контроля.

**Содержание**:

1. В чем сложности с мобильными платформами?

Традиционный способ: «завернуть гайки» — не очень работает. Во-первых, для BYOD мобильное устройство принадлежит пользователю. И он совсем не обязан и не желает отдавать полный контроль организации. И производители платформ с ним в этом солидарны.

Выверенная система безопасности современных ОС строится на доверии компонент от «железа» до конечного приложения. Решаете нарушить систему (получив root или сделав jailbreak) – и на средства безопасности ОС уже нельзя положиться.

Разные платформы имеют собственные правила и ограничения. Попытки сделать детальную политику безопасности на все платформы с высокой долей вероятности обречены на провал: на Android можно запретить делать скриншот из приложения, а на iOS – нет. На iOS можно заставить доверять всей системе частному издателю, а на Android – только не для системного контекста. На Windows удаленное управление экраном не проблема, а на iOS – невозможно.

1. iOS
   1. BYOD

Архитектурно приложения выполняются изолированно и не имеют расширенных прав в системе. Забудьте о приложении-агенте-администраторе. Управление только через MDM API.

Последнее слово всегда за пользователем: захотел – принял профиль. Захотел – удалил.

Можно распространять профили доступа (сертификаты, VPN (в т.ч. per-app), WiFi, email). При этом даже предоставляется базовое разграничение контекста – переслать рабочее письмо через личную почту не даст. И открытие вложения регулируется политикой. НО нет контроля буфера обмена.

Если приложение уже установлено, его можно «перехватить». Станет управляемо организацией и сотрется вместе с профилем.

Можно отозвать профиль. А также сделать factory reset.

* 1. В версии iOS 13 появляется поддержка User Enrollment – попытка сделать BYOD более качественно разделенным. В этом режиме профиль управления устройством не устанавливается, а на устройство приезжает отдельная учетная запись (Apple Business Manager), которая создает изолированный рабочий контекст: можно ставить приложения, профили VPN, настройки. Доступа к устройству и личной информации нет. Увы…. Apple Business Manager не доступен (как и остальные корпоративные программы Apple) в России.
  2. Supervised. Если организация приобретает устройства, она имеет право на более жесткий контроль. Этот режим называется Supervised и позволяет получать больше информации и контроля: включать режим киоска, переводить в режим пропажи, находить координаты, вводить наиболее жесткие ограничения на устройстве. Два способа включения: перезаливка через Apple Configurator или приобретение по корпоративной программе DEP. Может настраиваться в связке и без связки с пользователем... Увы, второй вариант требует Apple VPP для установки даже бесплатных приложений. И потому не доступен в России.

1. Mac OS X
   1. Предоставляет возможности базового управления устройством без особых сюрпризов.

В этом режиме разделяется управление пользователем и системой. MDM API позволяет настраивать требования к паролю, конфигурировать средства безопасности (Шифрование диска, фаервол, политики безопасности), Сертификаты, VPN, Wi-Fi, установка приложений как из магазина, так и sideloading, возможность очистить устройство. Для автоматической регистрации в MDM, а также некоторых расширенных настроек (например управление обновлениями) требуется использование DEP. Который на территории России… Ну, в общем вы поняли.

1. Режимы и методы управления Android
   1. Device Admin

В 2010 году в составе Android 2.2 появился набор API Device Admin Mode, призванный обеспечить возможность корпоративного управления устройствами. Предполагалось, что MDM устанавливает свое приложение-агент, и дает ему расширенные полномочия: Параметры пароля, шифрование, блокировка, отключение камеры, установка приложений, VPN, сертификатов, сброс устройства. Все. Андроид без дополнительных модификаций больше вариантов не предлагает, но отдельные производители стали предлагать свой API поверх. В версии Android 9 этот API объявлен deprecated. В Android 10 – отключен. По-прежнему доступны лишь шифрование и сброс.

* 1. Android Enterprise

Ответом на эти проблемы стал представленный в Android 5.1 режим Android Enterprise. С версии 6.0 стал доступен на всех устройствах. API, позволяющий обеспечить разделение режима рабочего и персонального устройства. В этом варианте единственным каналом управления становится интегрированный MDM агент, и платформа четко разделяет полномочия. Для корпоративных устройств выделяется три основных режима администрирования:

- Company Owned Single Use (Dedicated device)- моноцелевые устройства с максимально строгими настройками (киоски, терминалы сборы данных).

- Корпоративные устройства с полностью контролируемой средой.

- Корпоративный устройства с наличием личного профиля.

Во всех вариантах поддерживается инвентаризация и контроль устройств, установка приложений (через Play for work), профили подключения и настроек. Требует включения устройства в этот режим определенным способом.

Для персональных устройств (по умолчанию) при подключении к MDM создается выделенное пространство Work Profile, в котором изолируются корпоративный данные, приложения, профили подключения. При этом администратор контролирует лишь рабочую область, а пользователь не может выводить данные за пределы рабочего профиля.

Отдельно хочется упомянуть разнообразие устройств. Т.к. подобный способ исключает отдельные агенты управления, для поддержки специализированных параметров и сборок предлагается OEM Config: производитель устройства размещает приложение-агент в магазине, которое понимает параметры контроля со стороны MDM. MDM разворачивает данное приложение и через политики App Config передает в него параметры настройки среды. Это позволяет отделить управление vendor-specific функционалом от управления ОС.

1. Режимы управления Windows 10.

С выходом Windows 10 MDM был объявлен основным каналом управления устройствами на данной ОС и лег в основу концепции Modern Management. Связка MDM + Azure AD Join позволяют реализовать не только управление в рамках современных стандартов управления устройствами с доступом в Интернет, но и технологию Autopilot - автоматическую настройку корпоративных устройств. Изначально configuration Service Providers обеспечивали настройку наиболее часто используемых параметров ОС. От версии к версии поддерживаемые политики расширялись, обеспечивая контроль параметров среды, настроек и технологий безопасности (антивирус, BitLocker, Exploit Guard, AppLocker, WIP и другие), установку различных приложений (Appx, exe, msi, MSIX) как из магазина, так и напрямую из MDM, распространение PowerShell скриптов позволяет закрыть любые недоступные иными средствами параметры конфигурации. Поддерживается распространение сертификатов, профилей подключения, режимы киоска, а также инструменты Embedded tools (для редакции Enterprise).

В рамках попыток обеспечить поддержку BYOD, Windows Pro и Enterprise поддерживают режим MAM without Enrollment – возможность применить политику Windows Information Protection при добавлении рабочей учетной записи. Что разграничит личные и корпоративные данные, обеспечив администраторов организации инструментами контроля и защиты данных организации на неуправляемом устройстве. К сожалению, требование Pro редакции и невозможность отсечь Home не позволяет использовать данный режим как самостоятельное решение для BYOD сценариев.

Подводя итоги, можно сформулировать следующие рекомендации:

1. Правильно выбирайте платформу и режим работы. Не всегда требования реализуемы на всех платформах и всех режимах.
2. При выборе платформы управления учитывайте целевые платформы и режимы. RFI без указания платформы не будет отражать объективной картины, т.к. скорее всего будет совмещать максимальный набор возможностей для всех платформ и режимов.
3. Часть заявленных возможностей не будут доступны. Наиболее яркий пример платформы Apple, где часть критичных режимов недоступны из-за отсутствия поддержки корпоративных программ в регионе.
4. По крайней мере в BYOD, MDM лишь часть решения, которая не всегда может обеспечить полный контроль корпоративной информации. Для успешной защиты также может требоваться контроль приложений или контекста в приложении.