IBM MaaS360 Mobile Application Management

Простота развертывания, управления и защиты мобильных приложений

Основные преимущества

- Защита корпоративных приложений с помощью контейнеров
- Повышение производительности труда и удовлетворенности сотрудников
- Централизованное управление мобильными приложениями с помощью веб-консоли
- Безопасная поддержка концепция использования собственных устройств сотрудников (BYOD)
- Снижение риска утечки конфиденциальных данных
- Обеспечение контроля доступа к устройствам и соответствия политикам и нормативным требованиям
- Выполнение выборочной очистки каталога приложений и управляемых приложений
- Использование детализированных средств административного контроля и интерактивных, графических отчетов
- Уменьшение нагрузки на сеть, повышение производительности и масштабируемости приложений

Предоставление защищенного доступа к приложениям

Смартфоны и планшеты преобразуют бизнес, повышая производительность труда сотрудников, эффективность работы и удовлетворенность клиентов. Однако распространение мобильных устройств не должно быть бесконтрольным. Необходимо защитить конфиденциальные корпоративные данные, особенно в эпоху BYOD (использование собственных устройств сотрудников).

Речь более не идет лишь о контроле электронной почты и управлении устройствами. Истинный потенциал мобильных устройств раскрывается в мобильных приложениях.

Однако, мобильные приложения все чаще становятся источником уязвимостей для безопасности предприятия из-за неправильного хранения данных, вредоносных программ, несанкционированного доступа, отсутствия шифрования и утечки данных при синхронизации.

Существует более миллиона различных мобильных приложений, которые ваши сотрудники могут установить и использовать на своих смартфонах и планшетах.[1]

Предприятиям необходима возможность распространять, управлять и защищать важные для бизнеса мобильные приложения как на личных, так и на корпоративных устройствах.

IBM® MaaS360® Mobile Application Management упрощает управление мобильными приложениями, предоставляя интуитивно понятный каталог корпоративных приложений с надежной защитой и оперативным управлением жизненным циклом приложений.

«К 2017 году на 25 % предприятий будет хранилище корпоративных приложений для управления разрешенными приложениями на ПК и мобильных устройствах»[2] – Gartner

Каталог корпоративных приложений

- Интуитивно понятный, настраиваемый каталог корпоративных приложений для устройств iOS, Android и Windows Phone
- Исключительные возможности для пользователей
- Моментальная справка, позволяющая пользователям просматривать доступные приложения, устанавливать их и получать оповещения об обновлениях
- Распространение избранных общих и корпоративных приложений
- Использование защищенной веб-консоли для управления и распространения приложений

Рис. 1. Пример каталога корпоративных приложений на мобильном устройстве

Управление жизненным циклом мобильных приложений

- Использование лучших разработанных на практике рабочих потоков для управления мобильными приложениями
- Распространение приложений и отслеживание их беспроводной установки (OTA) на устройства всех пользователей, групп пользователей или на отдельные устройства
- Публикация обновлений приложений
- Справочные отчеты по инвентаризации приложений
- Интеграция с общими магазинами приложений, такими как Apple App Store, Google Play и Windows Phone Store, для обеспечения простых рабочих потоков.

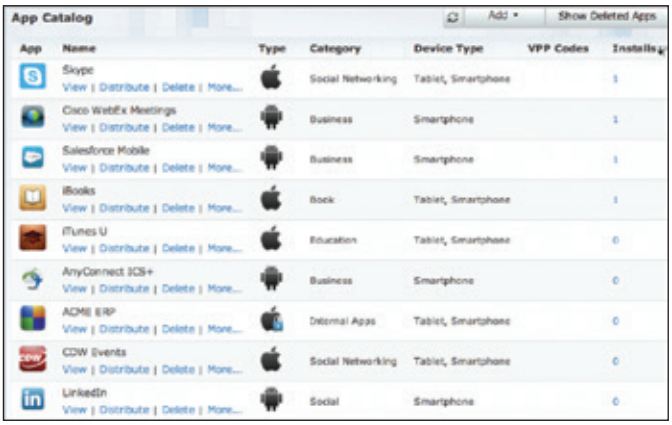

Рис. 2. Пример каталога приложений на портале MaaS360

IBM® MaaS360® Mobile Application Security

- Использование простой оболочки приложений или комплекта SDK в качестве дополнительного модуля защиты для MaaS360 Mobile Application Management
- Аутентификация пользователей перед доступом к приложениям
- Принудительная проверка устройства на соответствие требованиям
- Ограничение копирования и вставки, а также создания резервных копий данных в локальной системе и облаке
- Получение предупреждений о нарушениях соответствия требованиям практически в реальном времени
- Создание туннелей на уровне приложений для защищенного доступа к корпоративным данным без использования VPN устройств

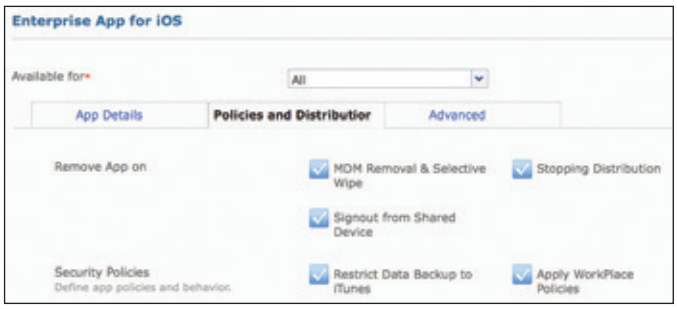

Рис. 3. Пример вариантов защиты, которые можно настроить для приложения

Соответствие требованиям к мобильным приложениям и обеспечение их соблюдения

- Черный список, белый список и набор необходимых приложений
- Ограничение встроенных приложений на устройстве (например, YouTube)
- Ограничение доступа для устройств под управлением суперпользователя и устройств с несанкционированно измененной микропрограммой
- Настройка автоматических действий принудительного контроля соответствия требованиям
- Моментальное выполнение действий благодаря автоматизации или выполнение действий вручную для блокировки доступа к электронной почте, ограничения сетевых ресурсов (например, отсутствие VPN) и выполнение дистанционной очистки
- Просмотр графических отчетов по безопасности и истории выполнения нормативных требований

Рис. 4. Пример помещения приложения в черный список. В результате его нельзя установить на устройстве

Контейнер корпоративных мобильных приложений

MaaS360 Mobile Application Management упрощает управление мобильными приложениями, предоставляя удобный каталог корпоративных приложений с надежной защитой и оперативным управлением жизненным циклом приложений.

Каталог корпоративных приложений
Интуитивно понятный, настраиваемый каталог корпоративных приложений для iOS, Android и Windows Phone.

Управление жизненным циклом мобильных приложений
Платформа для распространения, обновления, управления и защиты общих и корпоративных мобильных приложений.

MaaS360 Mobile Application Security
Контейнер для мобильных приложений предприятия с встроенными средствами управления безопасностью в качестве дополнительного модуля для MaaS360 Mobile Application Management.

Соответствие требованиям к мобильным приложениям и обеспечение их соблюдения
Политики безопасности для черного списка, белого списка и необходимых приложений. Автоматическое выполнение правил для оповещения администраторов, блокировки электронной почты, ограничения сетевых ресурсов и выполнения дистанционной очистки.

IBM® MaaS360® Content Service
Возможность размещения и распространения корпоративных мобильных приложений по оптимизированной в глобальном масштабе сети распространения приложений.

Программа оптовой покупки
Поддержка пакетных лицензий на приложения для сотрудников.

Дополнительные сведения о решениях IBM Security для предотвращения мошенничества можно получить у представителя компании IBM или ее бизнес-партнера, а также на следующем веб-сайте: **ibm.com**/security.

IBM Восточная Европа/Азия
123317, Москва
Пресненская наб., 10
Тел.: +7 (495) 775-8800
Факс: + 7 (495) 258-6468, 258-6404
ibm.com/ru

Подготовлено в США.
Январь 2016 г.

Этот документ актуален на дату первоначального опубликования и может быть изменен IBM в любое время. Некоторые предложения могут быть недоступны в странах, где IBM ведет свою деятельность.

Данные о производительности и примеры заказчиков приведены в документе только в качестве иллюстрации. Фактическая производительность может зависеть от конкретной конфигурации и условий эксплуатации. Ответственность за оценку и проверку работы любого другого продукта или программы вместе с продуктами и программами IBM лежит на пользователе.

ИНФОРМАЦИЯ В НАСТОЯЩЕМ ДОКУМЕНТЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИИ ИЛИ УСЛОВИЯ КОММЕРЧЕСКИХ КАЧЕСТВ, ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ ИЛИ НЕНАРУШЕНИЯ ЧЬИХ-ЛИБО ПРАВ. Гарантия на продукты IBM определяется условиями и положениями соглашений, действующих для продуктов в момент продажи.

Ответственность за выполнение требований всех действующих законов и нормативов несут заказчики. Корпорация IBM не предоставляет юридических консультаций и не дает гарантии, что ее продукты и услуги соответствуют требованиям каких бы то ни было законов.

Заявления относительно направления действий и намерений компании IBM в дальнейшем могут быть изменены или аннулированы без предварительного уведомления и представляют собой только цели и задачи.

Заявление о добросовестных практиках безопасности. Безопасность ИТ-систем включает в себя защиту систем и информации путем предотвращения, обнаружения и реагирования на несанкционированный доступ в рамках предприятия и за его пределами. Несанкционированный доступ может приводить к изменению, уничтожению или неправомочному присвоению информации либо к повреждению или недопустимому использованию ваших систем, включая атаки на другие системы. Ни одна ИТ-система или продукт не может считаться абсолютно защищенным, и ни один продукт или мера безопасности не может быть полностью эффективной в предотвращении несанкционированного доступа. Системы и продукты IBM разрабатываются как часть комплексного подхода к обеспечению безопасности, который будет в обязательном порядке включать в себя дополнительные оперативные процедуры и для наиболее эффективного функционирования может требовать наличия других систем, продуктов или сервисов. Компания IBM не гарантирует неуязвимость этих систем и продуктов по отношению к злоумышленным или незаконным действиям любой стороны.

Подлежит переработке и вторичному использованию

1 Количество приложений, доступных в ведущих магазинах приложений, по данным на июль 2014 г., Statista, http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

2 «*Gartner утверждает, что к 2017 г. на 25 % предприятий будет магазин корпоративных приложений*»Gartner Group Press Release, 12 февраля 2013 г. http://www.gartner.com/newsroom/id/2334015

WGD03060-RURU-01