IBM Security
Описания – Передовые идеи

Практические рекомендации по управлению жизненным циклом мобильных приложений

Безопасность, начиная с проектирования и до развертывания

IBM

Роль безопасности при разработке мобильных приложений

Во многих организациях мобильные устройства стали реальностью. Организации на основе Mobile Device Management (MDM) и Mobile Application Mºanagement (MAM) увеличивают объем разработки собственных корпоративных приложений, предназначенных для выполнение специальных задач, увеличения производительности, укрепления деловых партнерских отношений, повышения степени удовлетворенности клиентов и общей эффективности компании. Но, чтобы воспользоваться этими преимуществами, необходимо на протяжении всего жизненного цикла приложения применять практические рекомендации по обеспечению безопасности мобильной среды.

Перед организациями стоит новая задача: как перенести практические рекомендации по обеспечению безопасности и соответствия нормативам на ноутбуки и другие мобильные устройства.

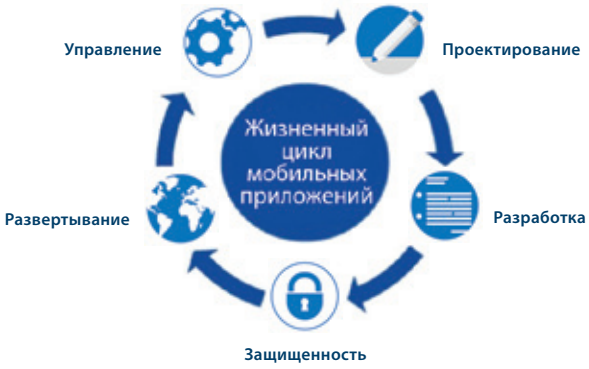

Рис. 1. Жизненный цикл мобильных приложений включает создание, защиту и управление приложениями

Решение Mobile Application Lifecycle Management (MALM) получило в наследство все проблемы, связанные с началом мобильной эры, в области обеспечения безопасности, соответствия нормативам и соблюдения конфиденциальности. Сюда входят обеспечение безопасности корпоративных и персональных данных, соответствия отраслевым стандартам и государственным требованиям и конфиденциальности сотрудников. Хотя разработка собственных мобильных приложений кажется сложной задачей, намного большую сложность вызывает защита приложений и связанных с ними данных.

IBM Security, признанный лидер в сфере управления мобильной средой предприятия (EMM), предоставляет лучшие практические рекомендации по обеспечению безопасности для этапов разработки и развертывания приложений. Предприятиям, на которых проектируются и разрабатываются собственные мобильные приложения, такие возможности предоставляются в составе средств разработки Software Development Kit (SDK) или в виде автоматического размещения приложений в оболочке.

Практические рекомендации по профилактическому обеспечению безопасности приложений

Наличие политики безопасности и ее применение после подготовки приложений к развертыванию – хорошая идея, но внедрение безопасности в процесс проектирования и разработки приложений позволяет с течением времени упростить работу и повысить ее эффективность. Помимо шифрования данных, которое обеспечивается операционной системой, устройства решение MaaS360 предоставляет несколько профилактических средств обеспечения безопасности, которые можно применять* во время разработки приложений. Среди этих функций:

Аутентификация

В дополнение к аутентификации устройств с помощью MaaS360, включающей базовую регистрацию с помощью пароля или двухфакторную аутентификацию, синхронизированную с Active Directory или LDAP, также можно встраивать средства аутентификации в приложения. Открывать специальные приложения и использовать связанные с ними данные смогут только те пользователи, у которых имеется доступ к этим приложениям, даже если такие приложения по ошибке попадают к другим пользователям.

Единый вход в систему

При разработке приложений можно предоставить пользователям возможность доступа ко всем авторизованным приложениям предприятия с помощью единого пароля. Такая функция поддержки MaaS360 обеспечивает ориентированный на пользователей подход при создании мобильных приложений с использованием таких платформ разработки как IBM Worklight*. Можно обеспечить строгую аутентификацию, не ухудшая

производительность работы пользователей. IBM® MaaS360® Trusted Workplace упрощает разработку приложений благодаря средствам аутентификации, единому входу в систему, предотвращению потерь данных (DLP), встроенному в приложения VPN и средствам блокировки приложений на различных мобильных платформах.

Предотвращение потерь данных (DLP)

MaaS360 поддерживает среду с двойным профилем, в которой на мобильных устройствах данные предприятия отделены от персональных данных. Разработчики и администраторы MDM могут различными способами использовать такой защищенный контейнер MaaS360 Trusted Workplace для защиты утечек данных, возникающих при смешивании данных предприятия и личных данных, и обеспечить конфиденциальность сотрудников.

- **MaaS360 Trusted Workplace:** Этот контейнер с шифрованием AES-256, совместимым с FIPS 140-2, обеспечивает защиту паролем и предоставляет доступ только после аутентификации владельца устройства. В случае потери или кражу устройства корпоративные приложения, документы и данные остаются защищенными. Помимо этого имеется возможность дистанционного удаления контейнера. Информация компании остается защищенной, даже если сотрудник сообщает в ИТ-отдел о потери своего устройства через несколько дней.
- **Выборочная очистка:** Из контейнера можно удалить практически всю информацию, размещенную с помощью MaaS360. При этом информация, загруженная пользователем для личного использования, сохраняется. (MaaS360 также предлагает возможность полной очистки и восстановления заводских настроек устройства.)
- **Ограничение возможностей копирования и вставки:** Решение MaaS360 позволяет отключить функцию копирования и вставки информация вне контейнера. Если пользователь попытается скопировать информацию из контейнера и вставить ее в ресурс, доступный из персонального профиля, например, в блокнот, собственное приложение электронной почты, веб-сайт с общим доступом к файлам или в облако с резервными копиями данных, вместо данных будет вставлено сообщение с напоминанием о политике безопасности предприятия. Также возможна автоматическая отправка уведомления администратору MaaS360.
- **Элементы управления открытием**: MaaS360 также предоставляет элементы управления открытием (open-in). То есть пользователи смогут открывать документы и файлы в приложениях, принадлежащих и управляемых компанией, только в контейнере MaaS360 Trusted Workplace. Информацию компании невозможно открыть вне контейнера. Также невозможно переместить ее вне контейнера.

Руководители и ИТ-сотрудники не могут непосредственно контролировать мобильные устройства, поэтому эти устройства в высокой степени уязвимы в отношении ошибок и неправильных действий сотрудников.

Встроенный в приложения VPN

Хотя все описанные выше меры повышают безопасность данных на мобильных устройствах, разработчикам приложений на предприятиях также необходимо обеспечить защиту оперативных данных, то есть информации, передаваемой из контейнера MaaS360 Trusted Workplace на серверы предприятия. Для защиты передаваемых данных необходимо VPN-соединение. Туннелирование на уровне приложений позволяет передавать данные пользователей по VPN-соединению на уровне приложения без использования VPN на уровне устройства. С помощью IBM® MaaS360® Gateway for Apps это можно сделать независимо от любой инфраструктуры VPN.

Блокировка приложений

Разработчики приложений также могут задать политики, которые блокируют открытие приложения пользователем на устройстве, несовместимом с функциями автоматического контроля безопасности.

Практические рекомендации для хранилища приложений предприятия

После разработки приложений для их распространения и управления рекомендуется использовать хранилище приложений предприятия. На самом деле многие заказчики MaaS360 уже используют функцию каталога приложений системы для управления общедоступными приложениями, например, приложениями из iTunes App Store, Google Play и Windows Store, а также собственными приложениями организации. Чтобы обеспечить более детализированный контроль приложений, контейнер MaaS360 Trusted Workplace можно использовать вместе с каталогом приложений MaaS360 App Catalog. Такой подход позволяет полностью отделить приложения, предоставляемые ИТ-отделом (собственные или сторонних поставщиков) от персональных приложений пользователей.

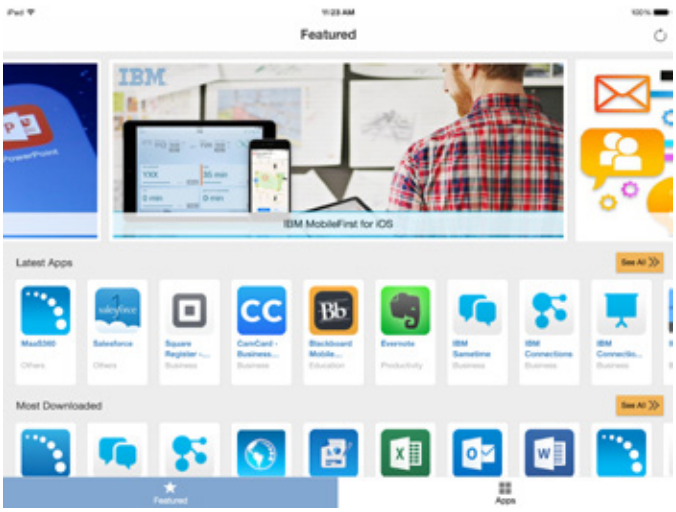

Рис. 2. Каталоги приложений позволяют легко найти утвержденные приложения

Преимущества полностью интегрированного хранилища приложений

Каталог MaaS360 App Catalog предоставляет консолидированный интерфейс, независимых от мобильной операционной системы. Это позволяет в одном окне управлять приложениями на различных платформах. Другие преимущества полностью интегрированного хранилища приложений:

Отсутствие задержек при развертывании и обновлении

Помимо специализированных приложений предприятия App Catalog интегрируется в общедоступными хранилищами приложений. Можно «по воздуху» распространять приложения и отслеживать их установку на отдельных устройствах, у групп пользователей или у всех пользователей посредством массового распространения. Если, к примеру, требуется предоставить приобретенное приложение iOS сотрудникам с помощью Apple Volume Purchase Program (VPP), можно загрузить файл VPP и управлять лицензиями с помощью MaaS360. Когда пользователь уходит из компании, это приложение можно удалить с устройства пользователя и перераспределить лицензии. Если пользователю требуется удалить и снова установить приложение, обращаться в ИТ-отдел, чтобы получить другую лицензию или посещать хранилище общедоступных приложений не требуется. Вместо этого можно просто перейти к каталог приложений App Catalog своей организации и нажать кнопку установки приложения.

Интеграция с существующей инфраструктурой предприятия обеспечению безопасности и хранению идентификационных данных

Во многих организациях требуется развертывать приложения для определенных групп пользователей. Хотя в MaaS360 можно настраивать группы, координация мобильной среды предприятия с существующими идентификационными данными пользователей в Active Directory или LDAP позволяет пропустить некоторые операции и обеспечить доставку необходимых приложений тем пользователям, которым они действительно нужны. Это можно сделать с помощью MaaS360 Cloud Extender. Чтобы настроить набор функциональных возможностей, для интеграции MaaS360 с ИТ-инфраструктурами различного типа рекомендуется использовать веб-службы. Это надежный, гибкий, эффективный и простой способ доступа к Интернету, при котором обеспечивается защита приложений, документов и данных.

Надежный контроль средств безопасности и управления приложениями

Если используется управление с помощью MaaS360, для специализированных приложений предприятия обеспечивается такая же защита, как и для других приложений. (См. следующий раздел о практических рекомендациях по обеспечению «пассивной» безопасности приложений.)

Контроль версий приложений

В случае общедоступных приложений для всех пользователей обычно доступна одна версия приложения. В случае корпоративных приложений, разработанных самостоятельно или сторонними организациями, перед распространением в рамках всей организации новую версию приложения можно предоставить только некоторым пользователям. Система MaaS360 позволяет развертывать различные версии одного приложения и управлять ими.

Обнаружение приложений и коллективная работа

Требуется предоставить пользователям возможность обнаруживать и получать авторизованные приложения, рекомендованные организацией или необходимые для выполнения работы. Компонент App Discovery Portal решения MaaS360 с помощью простого интерфейса позволяет легко обнаруживать приложения. Пользователи также могут безопасно делиться или предоставлять ссылки на приложения, утвержденные для использования в контейнере Trusted Workplace. Также пользователи могут комментировать и оценивать приложения. Это помогает определить степень полезности приложений и выявить, приложения, которые необходимо обновить или дополнить для повышения эффективности работы.

Управление приложениями и отчетность по требованию

По требованию администратор MaaS360 может просматривать и создавать отчеты для всех приложений в App Catalog, для авторизованных пользователей и для приложений в контейнере WorkPlace на устройстве каждого пользователя. Администратор может удалять приложения у любого пользователя, группы или на всех устройствах, например, можно удалить предыдущую версию при обновлении приложения.

Становятся доступными все более сложные продукты, позволяющие контролировать и регистрировать передачу важных файлов на устройства хранения и на другие компьютеры по электронной почте, с помощью функции передачи файлов или с помощью приложений для мгновенного обмена сообщения. Также можно полностью заблокировать такую передачу файлов.

Одна платформа для простой работы и повышения безопасности

С помощью IBM Worklight используйте одно окно для разработки приложений для вех мобильных платформ. С MaaS360 используйте одно окно для MDM, MAM и MALM для всех платформ. Такой интегрированный подход может повысить эффективность преимуществ мобильной среды предприятия, предоставив высоким уровень контроля, безопасности, соответствия нормативам и производительности с одновременным уменьшением потребностей в ресурсах, времени и бюджете.

Практические рекомендации по обеспечению «пассивной» безопасности приложений

Если используется управление с помощью MaaS360, для общедоступных и корпоративных приложений применяются одинаковые средства организационного контроля и защиты, например:

- Составление белых и черных списков приложений
- Конфигурации безопасности и ограничений
- Автоматические действия принудительного контроля при несоответствии (уведомление, блокировка устройства, выборочная или полная очистка)
- Автоматический контроль устройств с несанкционированно измененной микропрограммой, устройств под управлением суперпользователя и несовместимых устройств

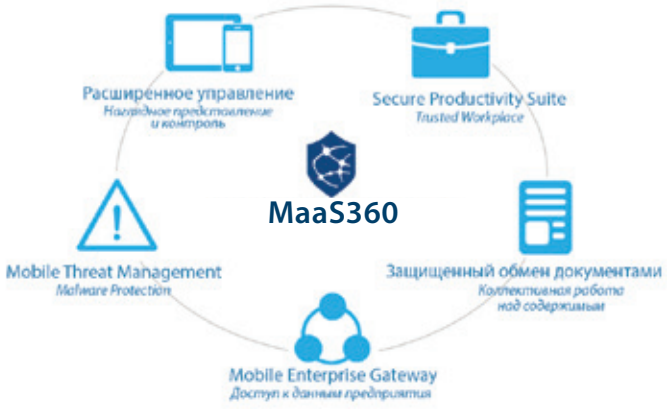

Рис. 3. Пять основных аспектов MaaS360

- Постоянная индикация состояния соответствия устройств нормативам
- Отчетность по журналу безопасности и соответствия

IBM® MaaS360® Secure Mobile Browser

Многие организации инвестировали значительные ресурсы и используют хорошо зарекомендовавшие себя бизнес-процессы, в основе которых лежат существующие бизнес-приложения. Решения MaaS360 Secure Mobile Browser и IBM® MaaS360® Gateway Suite позволяют предоставить сотрудникам защищенный доступ с мобильных устройств к сайтам внутренней сети предприятия и приложениям, например, к частным средам SharePoint, Windows File Sharing и внутренним веб-сайтам. Это позволяет перенести в мобильную среду все веб-приложения без необходимости перезаписывать их код для мобильной среды или полностью настраивать VPN на уровне устройств.

Решение MaaS360 Secure Mobile Browser также предоставляет администратору MaaS360 возможность ограничить доступ к веб-сайтам с любого из устройств на основе категорий и сделать исключение в бизнес-целях для устройств с ограниченным доступом. Например, если в организации используются черные списки социальных сетей, администратор может сделать исключение для специалиста по маркетингу или связям с общественностью и предоставить ему доступ к LinkedIn, если это требуется дл размещения бизнес-материалов. Если сотрудник пытается подключиться к социальным сетям, доступ блокируется. (Администратор может просмотреть журналы аудита с записями с указанием времени и даты, которые позволяют определить пользователя и устройства для каждой попытки получить доступ к веб-сайту с ограниченным доступом. Сотрудникам, повторяющим попытку доступа к запрещенным веб-сайтам, можно отправлять предупреждения с помощью системы обмена сообщениями MaaS360.)

IBM® MaaS360® Mobile Application Security SDK

MaaS360 Mobile Application Security SDK позволяет разработчикам всего лишь за несколько часов встроить в свои приложения надежные функции обеспечения безопасности MaaS360 в виде настраиваемого уровня безопасности. SDK позволяет разработчикам всего лишь за несколько часов встроить в свои приложения надежные функции обеспечения безопасности в виде настраиваемого уровня безопасности. Или же можно встроить эти функции обеспечения безопасности за несколько секунд при упаковке приложений. Возможность встраивания SDK во время разработки позволяет использовать для приложений предприятия все средства защиты MaaS360 в точном соответствии с потребностями приложений. SDK также позволяет разработчикам интегрировать MaaS360 с множеством различных функций, встроенных в устройства с iOS, Android и Windows Phone.

Мгновенная упаковка приложений MaaS360

Функция упаковки приложений MaaS360 добавляет необходимый код в уже разработанные приложения. Чтобы за несколько секунд добавить надежные средства MaaS360 для обеспечения безопасности и управления приложениями, нужно всего лишь нажать кнопку.

Еще один важный шаг на пути к мобильной среде предприятия

Процесс разрешения сотрудникам использовать своим устройства на предприятии занял несколько лет, в случае с MALM все происходит намного быстрее. Возможности мобильной среды предприятия с учетом стратегических задач и деятельности предприятия неоспоримы, когда речь идет о производительности, взаимодействии с клиентами и партнерами, степени удовлетворенности сотрудников и общей эффективности компании. С момента найма на работу и до интервью при увольнении мобильный телефон сотрудника по существу является основной точкой доступа к авторизованным цифровым и физическим ресурсам организации. Специализированные корпоративные мобильные приложения являются следующим важным шагом, к которому стремятся во многих организациях, где средства обеспечения безопасности мобильной среды обеспечивают защиту информации на уровне фиксированной ИТ-инфраструктуры. Во множестве организаций во всем мире решение MaaS360 уже помогает реализовывать мобильные инициативы в отношении MDM, MAM и MALM с помощью решений, простых для внедрения и управления ИТ-специалистами, удобных для пользователей и достаточно гибких для развивающегося мобильного мира.

О решении IBM MaaS360

IBM MaaS360 – это платформа управления мобильной средой предприятия, предоставляющая средства повышения производительности и защиты данных. Тысячи организаций рассматривают MaaS360 в качестве основы для своих мобильных инициатив. MaaS360 предоставляет инструменты комплексного управления с действенными средствами защиты пользователей, устройств, приложений и данных, обеспечивая поддержку развертывания любых мобильных сред. Чтобы узнать подробнее о решении IBM MaaS360 и начать 30-дневный бесплатный период пробного использования, посетите веб-сайт www.ibm.com/maas360

О подразделении IBM Security

Платформа обеспечения безопасности IBM предоставляет средства интеллектуального анализа безопасности и помогает организациям сформировать целостную защиту сотрудников, данных, приложений и инфраструктуры. Компания IBM предоставляет решения для управления идентификацией и доступом, управления информацией и событиями безопасности, защиты баз данных, разработки приложений, управления риском, управления конечными точками, защиты от вторжений и так далее. Компания IBM поддерживает работу одной из крупнейших в мире организаций, занимающихся исследованиями, разработкой и предоставлением решений по безопасности. За дополнительной информацией обращайтесь на веб-сайт по адресу www.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.
Март 2016 г.

Подлежит переработке и вторичному использованию

WGW03110-RURU-01