



Основные преимущества

- Безопасная поддержка концепция использования собственных устройств сотрудников (BYOD)
 - Разделение личных и корпоративных данных
 - Снижение риска утечки конфиденциальных данных
 - Использование единого входа в систему для аутентификации
 - Поддержка проверок соответствия требованиям при подключении к сети и в автономном режиме
 - Контейнер электронной почты, корпоративные профили или устройство в целом
 - Простой, интуитивно понятный интерфейс пользователя, не замедляющий работу сотрудников
 - В MaaS360 нет доступа к конфиденциальным данным электронной почты
 - Не интегрируется с данными электронной почты, не создает риск простоя или снижения производительности
-

IBM MaaS360 Secure Mobile Mail

Управление корпоративной электронной почтой на мобильных устройствах

Предоставление защищенного доступа к корпоративной электронной почте

IBM® MaaS360® Secure Mobile Mail предоставляет защищенное офисное приложение с электронной почтой, календарем и списком контактов, которое позволяет сотрудникам безопасно взаимодействовать с коллегами и использовать мобильные возможности персональных устройств.

Являясь одним из основных компонентов IBM® MaaS360® Productivity Suite, это решение устраняет основные опасения, связанные с рисками потери данных.

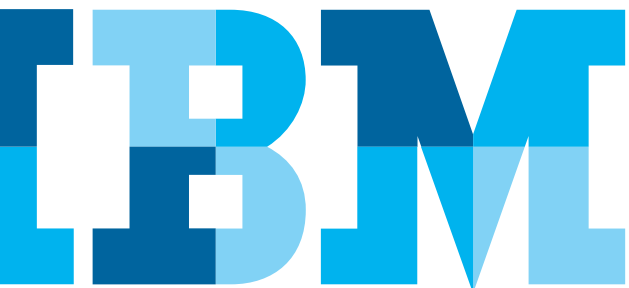
Благодаря аутентификации и авторизации, только одобренные и зарегистрированные пользователи могут обращаться к конфиденциальным электронным письмам и данным. Политики, контролирующие потоки данных, позволяют ограничить обмен данными между пользователями, перенаправление вложений, копирование и вставку данных. Утерянные, украденные или скомпрометированные устройства могут избирательно очищаться для удаления защищенного контейнера электронной почты, всех вложений и профилей.

Выберите правильный подход к защите электронной почты

Другие решения защищают электронную почту, перехватывая поток сообщений, удаляя вложения и загружая их в отдельное приложение. Обычно это ведет к разобщению работы пользователей с встроенным почтовым клиентом и автономными приложениями, которые могут обеспечить всего лишь просмотр документов.

MaaS360 Secure Mobile Mail гармонично работает в комплекте MaaS360 Productivity Suite, который обеспечивает управление всей электронной почтой, календарями, списками контактов, документами и работой в Интернете из одного изолированного рабочего пространства на мобильных устройствах.

Для пользователей обеспечиваются согласованные возможности при работе с электронной почтой, просмотре, редактировании и обмене документами.



Надежное приложение электронного секретаря (PIM)

- Защита электронной почты, календаря и списка контактов
- Обеспечение аутентификации и блокировка несанкционированного доступа к электронной почте
- Управление сообщениями электронной почты и вложениями с контейнере
- Просмотр вложений непосредственно в приложении
- Возможность не только просматривать, но и создавать, редактировать, сохранять контент и обмениваться им в зашифрованном комплекте IBM® MaaS360® Content Suite
- Работа со стандартными типами файлов, включая Word, Excel, PowerPoint, текстовые файлы и PDF

Мощная защита от утери данных

- Контроль возможных местоположений для копирования или перемещения файлов
- Ограничение перенаправления и перемещения в другие приложения
- Блокировка копирования, вставки и создания копий экрана
- Защита не только вложений электронной почты, но и текстов электронных сообщений
- Принудительная проверка устройства на соответствие требованиям
- Выборочное удаление контейнера и вложений, даже за пределами электронного почтового ящика

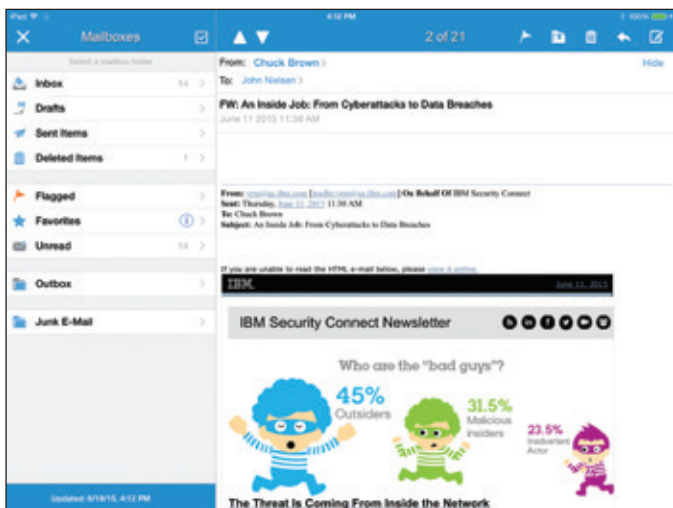


Рис. 1. Пример внешнего вида контейнера, папки «Входящие» и электронного письма на устройстве

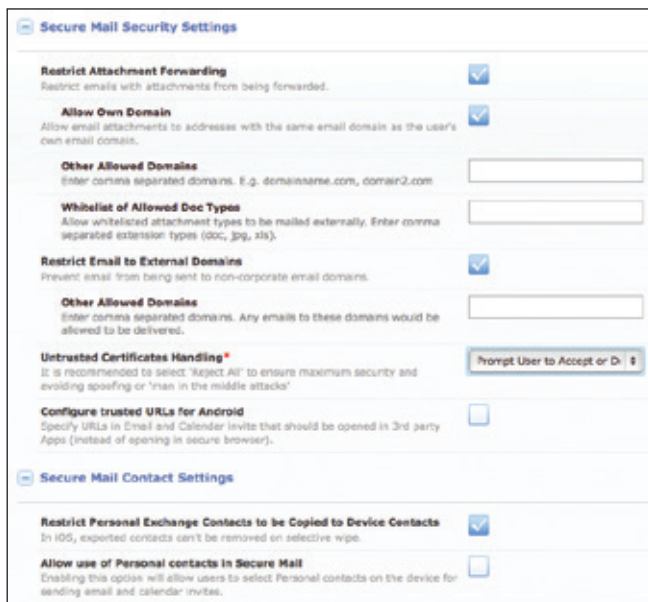


Рис. 2. Пример параметров безопасности для MaaS360 Secure Mobile Mail

Легкость интеграции в имеющуюся инфраструктуру

- На основе существующей инфраструктуры Exchange ActiveSync
- Использование Active Directory для упрощения аутентификации и авторизации
- Поддержка облачных механизмов электронной почты, таких как Office 365 и Gmail
- Интеграция надежной системы защиты электронной почты на уровне устройств без интеграции с данными электронной почты
- В MaaS360 нет доступа к конфиденциальным данным электронной почты
- Нет дополнительных рисков простоя или снижения производительности

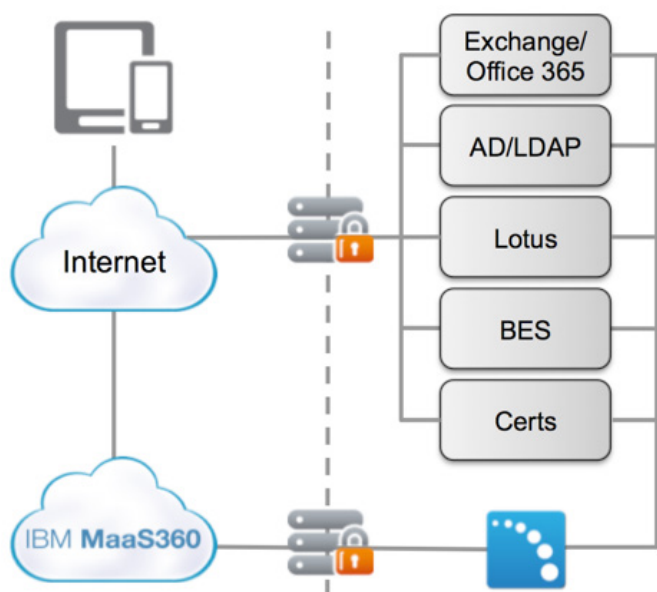


Рис. 3. Упрощенное представление интеграции MaaS360 с ИТ-системами

Постоянные оповещения и отчеты по безопасности

- Настройка автоматических действий принудительного контроля соответствия требованиям
- Автоматические оповещения о несоответствии требованиям
- Незамедлительное вмешательство в процессы, ручное или автоматическое
- Просмотр графических отчетов по безопасности и истории выполнения нормативных требований

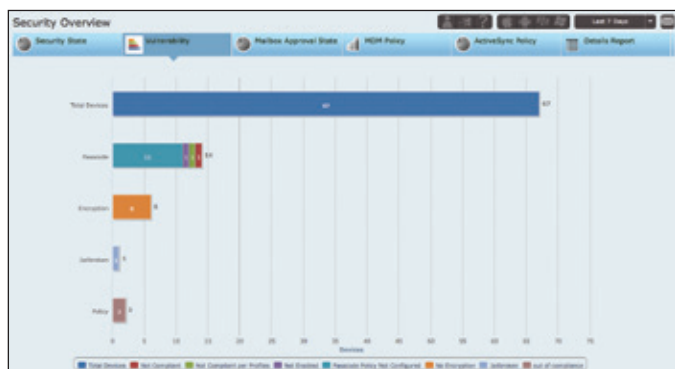


Рис. 4. Пример отчетов по безопасности MaaS360

Контейнер корпоративной электронной почты

Электронная почта по-прежнему является одним из необходимых приложений на смартфонах и планшетах, однако также может создавать сложности для политик организации в отношении защиты мобильных устройств и приложений и соответствия нормативным требованиям.

MaaS360 Secure Mobile Mail защищает электронную почту и вложения, предотвращая утечки корпоративных данных и поддерживая эффективность работы мобильных сотрудников.

Основные функции

- Защита электронной почты (текстов и вложений), календарей и списков контактов в контейнере
- Обеспечение аутентификации и блокировки несанкционированного доступа к электронной почте
- Выполнение проверок соответствия требованиям при работе в сети и в автономном режиме перед доступом к электронной почте
- Использование соответствующего FIPS 140-2 шифрования AES-256 для устройств iOS и Android
- Просмотр вложений непосредственно в приложении
- Контроль возможных местоположений для копирования или перемещения файлов
- Ограничение перенаправления, перехода к другим приложениям, копирования, вставки и создания снимков экрана
- Выборочное удаление вложений, даже за пределами электронного почтового ящика
- Работа в комплекте MaaS360 Content Suite для хранения, просмотра, редактирования контента и обмена им

Чтобы узнать подробнее о решении IBM MaaS360 и начать 30-дневный бесплатный период пробного использования, посетите веб-сайт www.ibm.com/maas360



© Copyright IBM Corporation 2016

ИВМ 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.
Февраль 2016 г.

ИВМ, логотип ИВМ, ibm.com и X-Force являются товарными знаками International Business Machines Corporation, зарегистрированными во многих юрисдикциях мира. BYOD360™, Cloud Extender™, Control360°, E360°, Fiberlink®, MaaS360°, MaaS360° и устройство, MaaS360 PRO™, MCM360™, MDM360™, MI360°, Mobile Context Management™, Mobile NAC°, Mobile360°, MaaS360 Productivity Suite™, MaaS360° Secure Mobile Mail и MaaS360° Content Suite, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360° и We do IT in the Cloud.™ и устройство являются товарными знаками или зарегистрированными товарными знаками Fiberlink Communications Corporation, компании ИВМ. Другие названия продуктов и услуг могут являться товарными знаками ИВМ или других компаний. Текущий список товарных знаков ИВМ доступен в разделе «Авторские права и товарные знаки» на веб-сайте по адресу ibm.com/legal/copytrade.shtml

Apple, iPhone, iPad, iPod touch и iOS являются товарными знаками или зарегистрированными товарными знаками компании Apple Inc. в США и других странах.

Microsoft, Windows, Windows NT и логотип Windows являются товарными знаками Microsoft Corporation в США и (или) в других странах.

Этот документ актуален на дату первоначального опубликования и может быть изменен ИВМ в любое время. Некоторые предложения могут быть недоступны в странах, где ИВМ 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 ИВМ 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 ИВМ определяется условиями и положениями соглашений, действующих для продуктов в момент продажи.

Ответственность за выполнение требований всех действующих законов и нормативов несут заказчики. Корпорация ИВМ 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 ИВМ 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 неправоначальному 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 ИВМ 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 ИВМ не гарантирует неуязвимость этих систем и продуктов по отношению к злоумышленным или незаконным действиям любой стороны.



Подлежит переработке и вторичному использованию