МОБИЛЬНОСТЬ В КОРПОРАТИВНЫХ ИТ-СИСТЕМАХ

ЯРОСЛАВ БОЦМАН

Представление о рабочей среде в современной корпоративной культуре претерпевает значительные изменения. Традиционный подход к повышению производительности и эффективности труда не позволяет продолжать его увеличение организационными методами. В настоящий момент происходят эволюционные изменения в рабочих инструментах, призванных усовершенствовать обработку информации.

Современные технологии создания, хранения, передачи и использования данных позволяют придать рабочему процессу большую динамичность и гибкость. Все чаще для поддержки корпоративных приложений используется концепция облачных сервисов.

Совершенствование технологичности рабочего процесса приводит к бурному росту клиентских приложений, предоставляющих пользователям «дружественный» интерфейс, рассчитанный на применение не только в ноутбуках, но и мобильных устройствах, в первую очередь — планшетах и смартфонов. Необходимость организации безопасного доступа к внутренним ресурсам компании из любых географически разнесенных мест требует контроля над мобильными гаджетами со стороны ИТ-администраторов предприятия. Парк корпоративных ПК пополняется менее динамично по сравнению с личными устройствами и зачастую не успевает за функциональными требованиями по удобству использования. Такая ситуация привела к возникновению концепции BYOD (Bring Your Own Device), то есть использованию в корпоративной сети собственных устройств сотрудников.

Три основных проблемы

Применение устройств, не принадлежащих компании, начинается с создания условий для безопасного доступа к ресурсам. На этом этапе необходимо ответить на три следующих важных вопроса.

1. Кто подключается к сети?
2. Откуда подключается пользователь?
3. Какое устройство он использует?

Однозначный ответ на вышеприведенные вопросы позволяет гарантировать защиту критически важных данных, особенно в условиях размытости границ корпоративных приложений. При доступе пользователя к данным извне сети предприятия необходимо обеспечить его аутентификацию и шифрование используемого канала. Несмотря на очевидную простоту использования предустановленного браузера для веб-подключения все чаще находят применение специализированные VPN-клиенты. Большинство производителей выпускают собственные клиентские приложения, их установка осуществляется пользователями из общедоступного репозитория или внутреннего корпоративного портала.

Применение VPN-клиента, кроме основного функционала, позволяет осуществлять профилирование и оценку состояния устройства. С помощью профилирования можно динамически квалифицировать тип устройства и автоматически использовать необходимую политику безопасности. А оценка состояния гарантирует соответствие устройства заданным требованиям безопасности: инсталляция нужного ПО, антивирусных средств, необходимых обновлений и др.

Применение стороннего устройства в корпоративной сети предполагает классификацию данных и приложений по правам использования — личные и корпоративные. Личные данные — это, как правило, фотографии, видеозаписи, личная переписка и собственные документы. Персональная информация и приложения должны оставаться в неизменном виде, корпоративные политики информационной безопасности к ним не применяются. Средства выполнения политик направляются только на защиту документооборота предприятия, специализированного программного обеспечения, а также результатов его работы.

Перенос критически важных для бизнеса данных и приложений на стороннее устройство требует от концепции BYOD реализации полного цикла управления мобильными устройствами (Mobile Device Management — MDM).

Рис. 1 Жизненный цикл управления мобильными устройствами

На этапе инициализации гаджета происходит установка клиентского программного обеспечения и начальное подключение к сети. Через установленное ПО на устройство производится передача политик безопасности, настроек подключений и расширенных параметров. Проведенная процедура гарантирует соответствие используемого мобильного аппарата всем требованиям безопасности и готовит его к использованию.

Приложение, устанавливаемое на устройстве, отвечает не только за его настройку и применение политик, но и за средства совместной работы. В состав приложения может входить защищенный браузер и пакет офисных приложений для безопасной комфортной работы.

Во время эксплуатации устройства осуществляется контроль за организацией доступа к приложениям, парольной политикой и процедурами применения шифрования. На этом этапе управления мобильными гаджетами необходимо регулярно проводить аудит конфигурации и установку необходимых обновлений.

Параллельно выполняется мониторинг и управление мобильными устройствами в режиме реального времени, что дает возможность обнулить параметры безопасности, удалить критически важные данные и блокировать устройство при его потере или увольнении владельца.

Некоторые производители реализуют на устройстве шифрованный контейнер, в который помещаются корпоративные данные и приложения. Для доступа к контейнеру применяется особый код доступа. Обычно есть возможность задать максимальное число неправильных вводов кода, после чего вся информация в контейнере уничтожается. Этот механизм защищает сохраненные данные даже при отсутствии подключения к сетям передачи данных.

Расширенные возможности по управлению мобильным аппаратом позволяют проводить резервное копирование данных и осуществлять поддержку корпоративных пользователей вне зависимости от типа и производителя применяемого устройства.

Важным этапом является реализация процедуры вывода из эксплуатации. В этом случае устройство очищается от всей корпоративной информации и при необходимости обнуляется до заводских настроек.

Распределенная архитектура

Для реализации жизненного цикла управления мобильными устройствами традиционно применяется два типа архитектуры — распределенная и централизованная. Распределенная архитектура включает четыре обязательных компонента: MDM-шлюз, шлюз к корпоративным сервисам, сервер управления и база данных.

На мобильном устройстве устанавливается специализированное приложение. Его основная задача: установка соединений с MDM-шлюзом при получении доступа к глобальным сетям передачи данных и выполнение команд и политик, получаемых от сервера управления.

MDM-шлюз служит для терминации подключений мобильных устройств и осуществляет их настройку и мониторинг, синхронизацию корпоративной информации (почтовых сообщений, календарей, контактов, и т.д.) и является прокси-сервером для внутренних ресурсов.

Центральным компонентом распределенной архитектуры является сервер управления. Он содержит в своем составе шлюз к корпоративным сервисам и базу данных для хранения информации о настройках и политиках для всех мобильных устройств и осуществляет управление MDM-шлюзом. Также сервер управления предоставляет консоль администратора для мониторинга и управления мобильными устройствами.

В зависимости от технического решения производителя и масштабов внедряемой системы все четыре компонента могут быть реализованы на одном устройстве или разнесены на нескольких серверах.

Такое решение максимально ориентированно на приложения корпоративной сети, но не позволяют реализовать полный жизненный цикл управления устройствами. Для его выполнения используются разнообразные облачные сервисы, служащие дополнением к функционалу MDM-системы. Их примером могут служить сервисы производителя МДМ, выполняющих плановые обновления системы, серверы Apple mdm, применяемые для управления устройствами iOS, Office 365, предоставляющими инструмент для продуктивной работы, его аналог Google Cloud и многие другие.

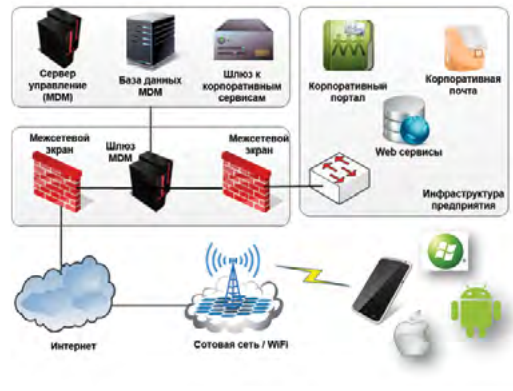

Рис. 2 Распределенная архитектура управления мобильными устройствами

Централизованная архитектура

В случае применения централизованной архитектуры МДМ-шлюз корпоративной сети выносится в облачный сервис производителя, а в корпоративной сети размещается сервер управления, содержащий в своем составе шлюз к корпоративным сервисам. Между компонентами строится зашифрованный туннель, в котором передается трафик из корпоративной сети к мобильному пользователю и осуществляется управление устройством.

Применение облачного сервиса в этом решении, предоставляет пользователям ряд преимуществ.

Все входящие подключения из сети интернет в сеть Заказчика терминируются в датацентре производителя. Это значительно снижает риски информационной безопасности за счет того, что к корпоративной сети получают доступ только запросы от аутентифицированных пользователей, а все атаки типа DoS выявляются и отражаются еще в датацентре.

Благодаря буферизации и специализированным решениям по оптимизации приложений в датацентре обеспечивается надежная доставка сообщений в условиях нестабильной работы сетей передачи данных, особенно при использовании сетей сотовой связи.

Кроме того, обеспечивается корректная работа с различными механизмами доступа к сети Интернет, которые используют разные операторы мобильной связи (примером может служить NAT, а также другие технологии). А отсутствие необходимости публиковать в Интернете серверы электронной почты и внутренние корпоративные ресурсы, к которым надо предоставлять доступ, дополнительно повышает защищенность сети.

Какой вариант выбрать?

Выбор архитектуры внедряемого решения основывается на соотношении требований по безопасности и уровня управляемости, как основных функциональных требованиях мобильных клиентов и администраторов сети. При необходимости реализации повышенных требований к безопасности корпоративных данных целесообразнее выбирать централизованное решение с расширенными возможностями по поддерживаемым приложениям. В случае акцента на управлении мобильными устройствами со средним уровнем защиты данных необходимо обратить внимание на системы с распределенной архитектурой.

Рис. 3 Централизованная архитектура управления мобильными устройствами

В настоящий момент решения большинства производителей позволяют реализовать как распределенную, так и централизованную систему управления мобильными устройствами. Это позволяет сформировать оптимальное решение из соотношений бюджета и возможностей управления уровнями безопасности и комфорта использования.

BYOD или не BYOD?

Используя привычные планшетные устройства и смартфоны, сотрудники будут иметь под рукой удобный и безопасный инструментарий. Они смогут проверять электронную почту после работы, заполнять формы запроса ресурсов, находясь у партнера, или согласовывать спецификацию закупаемых материалов, пребывая у заказчика.

Реализация концепции BYOD и внедрение системы управления мобильными устройствами сокращает время реакции пользователя на поставленную задачу, ведет к упрощению рабочих процессов и их оптимизации, что повышает конкурентные преимущества компании. Поэтому сегодня внедрение на предприятии концепции BYOD и системы управления мобильными устройствами — не вопрос выбора, а лишь вопрос времени.

Автор статьи —
главный консультант компании
«ЭС ЭНД ТИ УКРАИНА»