CompuWay

Enterprise mobility management: работа с концепцией BYOD с безопасной среде доставкой приложений и данных

Почему Citrix XenMobile является оптимальным подходом

CITRIX®

Введение

Преобразование компьютерной среды благодаря возможности доступа к ресурсам и приложениям с мобильных устройств, ориентации на потребителя, использованию собственных устройств сотрудников (BYOD) и гибкому подходу к работе предлагает серьезные преимущества современным организациям, однако одновременно ставит сложные задачи перед ИТ-отделами. Эти тенденции позволяют увеличить гибкость бизнеса, индивидуальную производительность и удовлетворенность работой, позволяя людям выбрать оптимальное время, место и устройства для выполнения своей работы. Чтобы реализовать такую гибкость, ИТ-отделы должны быть в состоянии обеспечить безопасность приложений и данных на потенциально неограниченном количестве разнообразных устройств, в любой сети, в любом месте, даже когда на тех же устройствах могут содержаться личные приложения и данные.

Поскольку для ИТ-отделов обеспечение безопасности имеет первостепенное значение, естественным стремлением для них будет попытаться уменьшить выбор устройств или иным образом ограничить среду конечных устройств, даже если при этом придется пожертвовать преимуществами повышения производительности и гибкости. Однако просто взять и отказаться от использования потребительских устройств и концепции BYOD невозможно и нежелательно – ИТ-отделы неизбежно столкнутся с нарастающей потребностью в обеспечении доступа к любому приложению, из любого места, на устройствах любого типа. Проще говоря, рано или поздно им придется реализовать и обеспечить поддержку потребительских устройств и концепции BYOD; остается лишь решить, как это сделать.

Первым ответом многих ИТ-организаций на приток мобильных устройств потребительского класса и мобильных устройств, принадлежащих сотрудникам, была попытка ограничения функциональности и взятия под контроль всех мобильных устройств на предприятии с помощью решений по управлению мобильными устройствами (MDM). MDM-решения могут быть весьма эффективным средством защиты конфиденциальной деловой информации: они контролируют используемые мобильные приложения, дистанционно стирают данные с утерянных или украденных устройств и обеспечивают другие важные функции. По мере быстрого увеличения разнообразия используемых мобильных устройств, операционных систем и приложений большинство ИТ-организаций, работающих с MDM, вынуждены налагать ограничения на мобильные приложения, имеющиеся на принадлежащих сотрудникам устройствах, во избежание повышения рисков безопасности и сложности управления. Другие типы приложений, включая приложения Windows®, веб- и SaaS-приложения, остаются недоступными, что ограничивает мобильную производительность. Хотя MDM подходит для сотрудников, выполняющих самые различные трудовые функции, многие подобные решения не обеспечивают гибкости, необходимой для реализации разнообразных вариантов применения в зависимости от индивидуальных требований к безопасности, соответствия требованиям регулирующих органов и функциональных возможностей мобильных устройств. В результате организации берут на вооружение новый подход, в котором MDM является лишь одним из компонентов более широкого комплекса возможностей, посредством которых ИТ-отделы могут управлять не только самими устройствами, но также имеющимися на них приложениями и данными. Такая система называется управлением корпоративной мобильностью (Enterprise Mobility Management, EMM), и она играет все более важную роль в новой эпохе информационных технологий.

Задача: диверсификация корпоративной вычислительной среды

Ориентирование на потребителей стирает границы между работой и личной жизнью, особенно когда речь заходит о мобильных устройствах. В настоящее время руководители и работники нового поколения обычно покупают смартфоны и планшеты для личного пользования и не видят никаких причин, по которым они не могли бы использовать их и для работы. В конце концов, в современной бизнес-среде работа – это то, что человек делает, а не место, где он это делает, и это может происходить в любом месте и в любое время дня или ночи. Основное внимание уделяется производительности, а не абстрактным понятиям вроде права собственности или ИТстандартов. Действительно, 67 % людей, использующих смартфоны для работы, и 70

% тех, кто использует для работы планшеты, выбирают устройства сами, не обязательно задумываясь о том, сможет ли их компания обеспечить соответствующую поддержку.[1] Они привыкли использовать устройство в различных условиях и не видят никакой разницы между использованием его для личных или рабочих целей.

Разумеется, это совсем не плохо. Любая компания хочет, чтобы ее сотрудники думали о повышении своей производительности и эффективности. Однако такая ориентированность на потребителей может стать проблемой для ИТ-организаций. По данным опроса Forrester Research, в 2016 году две трети планшетов будут проданы для личного пользования, и многие покупатели будут брать их с собой на работу.[2]

В связи с тем, что ИТ-отделы уже не могут выполнять свою привычную функцию по принудительному обеспечению стандартизации в этой сфере, на рабочих местах появляются самые разнообразные мобильные устройства: не только Apple iOS® и Google Android®, но также платформы сторонних разработчиков Android и Microsoft® Windows®. Как ИТ-отделы будут обеспечивать безопасность и контролировать все разнообразие мобильных устройств в условиях постоянного появления на рынке новых моделей и без ограничения гибкости по видам приложений, которые могут использоваться, и поддерживаемых функций? Ответ на этот вопрос – развертывание комплексного решения EMM, обладающего обширными возможностями для обеспечения безопасности и контроля не только над устройствами, но и над приложениями и содержащимися на них данными.

Управление мобильными устройствами: важный шаг к безопасности концепции BYOD

MDM может стать важным шагом для организаций, которым необходим контроль над потребительскими устройствами и их использованием в своей среде. Компания Citrix предоставляет эту возможность с помощью Citrix XenMobile MDM – системы, которая обеспечивает ролевое управление доступом, возможности конфигурации и безопасность для корпоративных и личных устройств сотрудников на протяжении всего срока службы устройства. ИТ-отделы могут регистрировать любое устройство и управлять им, обнаруживать устройства, работающие под управлением пользователя root, а также полностью или выборочно стирать данные с несоответствующих, утерянных, украденных или принадлежащих уволенным сотрудникам устройств. Средства обеспечения безопасности приложений включают: безопасный доступ к приложениям через туннельные соединения, черный список, белый список и динамичные контекстно-зависимые политики. Возможности сетевой безопасности обеспечивают прозрачность и защиту от внутренних и внешних мобильных угроз; блокировку неконтролируемых устройств, неавторизованных пользователей и несовместимых приложений; а также интеграцию с системами управления относящейся к безопасности информации и событиям (SIEM). В результате ИТ-отделы могут позволить сотрудникам самим выбрать устройство, которое те будут использовать, при условии его соответствия требованиям регулирующих органов и обеспечения безопасности хранимой на нем коммерческой информации.

Несмотря на высокую эффективность MDM, это лишь одна из составляющих комплексной стратегии для обеспечения безопасности потребительских устройств, используемых в рабочих целях. Многие мобильные приложения имеют недопустимые слабые места в системе обеспечения безопасности, например те, что перемещают или хранят данные в сторонних облачных сервисах. Простое занесение таких приложений в черный список для всех пользователей ограничит имеющиеся на предприятии возможности. Более оптимальным подходом будет обеспечение контроля над защитой, хранением и использованием данных в пределах этих приложений, что даст ИТ-отделам возможность разрешать их использование в определенных случаях. Что еще важнее, мобильные приложения являются лишь одним из элементов популярного в настоящее

[1] Опрос Forrsights Workforce Employee Survey, Q2 2012, Forrester Research, Inc., 2012. [2] Планшеты станут основным персональным компьютерным устройством будущего, Forrester Research, Inc., 23 апреля 2012 года.

время мобильного стиля работы. Чтобы раскрыть все преимущества мобильности пользователей, ИТ-отделы должны иметь достаточную гибкость для установки любого приложения – мобильного, веб-приложения, приложения Windows или SaaS – на любой тип устройства при условии обеспечения полной безопасности, соответствия стандартам предприятия, а также удобства и продуктивности для пользователей. Без доступа к этим возможностям MDM становится всего лишь еще одним промежуточным решением в среде постоянно усложняющейся и трудно поддающейся контролю мобильной инфраструктуры.

Выходя за рамки MDM: управление корпоративной мобильностью

Компания Citrix – лидер в области мобильности – разработала новый подход, позволяющий сотрудникам использовать мобильные устройства на их выбор, обеспечивая при этом эффективную безопасность и контроль над корпоративными приложениями и данными. Благодаря использованию не зависящей от устройства технологии, которая позволяет доставлять Windows-приложения на любое устройство, в любом месте и для всех пользователей, большинство клиентов Citrix уже использует решения Citrix XenDesktop, Citrix XenApp и Citrix NetScaler для поддержки мобильных пользователей и удаленных сценариев использования. Теперь компания Citrix воспользовалась этим опытом и проверенными технологиями для создания полной системы управления мобильными устройствами предприятия, которая позволяет ИТ-отделу доставлять все приложения, включая мобильные, веб-приложения, приложения SaaS и Windows, а также данные на любые устройства.

Суть подхода Citrix к управлению корпоративной проста: дать возможность ИТотделам управлять не только устройствами, но также приложениями и данными в рамках предложения от одного разработчика. Компания Citrix реализует EMM посредством Citrix XenMobile™, что позволяет радикально упростить доставку и управление приложениями, данными и ИТ-услугами. XenMobile позволяет ИТ-отделам создать на любом устройстве безопасный контейнер для изоляции корпоративных приложений и данных от личного контента. Такой контейнер обеспечивает полный контроль над всем корпоративным контентом посредством автоматизированных политик использования и прямых решений по администрированию, обогащая и насыщая опыт пользователя. Все содержимое безопасного контейнера можно дистанционно заблокировать и при необходимости удалить для обеспечения соответствия требованиям регулирующих органов. Эти особенности позволяют ИТ-отделам обеспечить безопасность и защиту корпоративного контента, даже если организация не является владельцем устройства. В XenMobile используются технологии Citrix MDX™, которые безопасно доставляют «родные» приложения iOS, Android и мобильные веб-приложения в безопасный контейнер, также обеспечивая полноценные возможности мобильных устройств для пользователей и полный контроль для ИТ-отделов. MDX-технологии включают в себя следующее:

- **Хранилище MDX Vault** – MDX Vault отделяет корпоративные мобильные приложения и данные от личных приложений на мобильных устройствах и помещает их в безопасный контейнер. С помощью MDX Vault ИТ-отделы могут управлять и контролировать «родные» мобильные бизнес-приложения и данные вместо управления самим принадлежащим сотруднику устройством. Безопасность бизнес-приложений в хранилище MDX Vault может быть обеспечена посредством шифрования и мобильных технологий DLP. ИТ-отделы могут дистанционно блокировать и удалять бизнес-приложения.
- **MDX Interapp** – решение для интеграции приложений MDX. MDX Interapp гарантирует, что все MDX-приложения могут взаимодействовать друг с другом для обеспечения оптимальной работы. Благодаря MDX Interapp приложения с поддержкой MDX интегрируются таким образом, чтобы такие приложения открывали только другие приложения с поддержкой MDX. Например, при нажатии на ссылку в электронной почте Citrix WorxMail автоматически запускается мобильный браузер Citrix WorxWeb, а не Safari. Также MDX Interapp контролирует взаимодействие между приложениями, чтобы ИТ-отделы могли назначать правила для различных действий, таких как

копирование и вставка данных: например, разрешить копирование и вставку данных только между MDX-приложениями, но не в других приложениях, или запретить включение камеры, когда используется определенное MDX-приложение.

- **MDX Access** – средство доступа MDX Access обеспечивает детальные средства управления и предоставления доступа на основе политик для всех «родных» мобильных приложений и приложений HTML5. ИТ-отделы могут централизованно контролировать и разрабатывать инструкции и правила специально для мобильных приложений, например тип используемого устройства или сети, код доступа устройства или действия при обнаружении устройства, работающего под управлением пользователя root. MDX Access также предоставляет первый в отрасли, зависящий от типа приложения доступ VPN во внутреннюю сеть компании. Использование micro-VPN позволяет предприятиям не использовать универсальный доступ VPN, который может ослабить систему безопасности. Вместо этого для удаленного доступа мобильных и веб-приложений к внутренней сети компании создается VPN-туннель под конкретное приложение.

С точки зрения управления информационными технологиями, средства управления на основе сценариев и провижининг на основе проверки личности пользователя помогают ИТ-отделам поддерживать безопасность и обеспечивать контроль независимо от времени, места и типа устройства, используемого для доступа к корпоративным приложениям и данным, на базе любой платформы. XenMobile использует существующие системы корпоративных каталогов и аутентификации для предоставления, доставки и контроля использования мобильных, интранет-, веб-, SaaS- и Windows-приложений и данных на основе идентификации пользователя и роли, а также анализа конечного устройства. ИТ-отделы могут мгновенно предоставить все приложения и данные пользователю, как только он добавляется в службу каталогов Active Directory. И наоборот, ИТ-отделы могут незамедлительно закрыть доступ определенным пользователям, отключив или удалив их из системы каталогов и закрыв их учетные записи.

Организационные преимущества управления корпоративной мобильностью убедительны, и для потребителя также имеются значительные преимущества. Например, XenMobile помогает ИТ-отделам внедрить единый магазин приложений. Эта растущая тенденция помогает предприятиям добиться более быстрой окупаемости приложений и уменьшить риски безопасности. Кроме того, ориентированная на пользователя архитектура магазина приложений сфокусирована на качестве использования и обеспечивает мгновенный доступ к приложениям и данным через красивый пользовательский интерфейс. Доступ к приложениям и данным, «которые следуют за мной», можно получить с любого устройства в любое время для обеспечения оптимальной производительности при различных сценариях использования. Технология единого входа в приложения повышает удобство и ускоряет работу. Таким образом, сотрудники не только могут использовать на работе устройство на свой выбор, но и получают возможности для достижения еще большей производительности, эффективности и удовлетворения от работы.

Управление корпоративной мобильностью в реальном мире

Клиенты Citrix уже используют XenMobile для решения задач управления мобильностью и обеспечения возможности использования всего разнообразия мобильных устройств.

Крупная **финансовая компания** использует XenMobile для поддержки комплексной мобильной стратегии. Эта организация заменила ряд точечных решений, обеспечивающих мобильность предприятия, на стандартную унифицированную платформу управления всеми приложениями и устройствами, включая мобильные. Корпоративные мобильные приложения включают MDX Access для обеспечения доступа к расположенным в интрасети приложениям в зависимости от уровня безопасности, географии и принадлежности к подразделению компании. «Родные» мобильные приложения доставляются в безопасный контейнер, чтобы отделить

бизнес-приложения и данные от личных материалов работника. Внедрив данную комплексную платформу управления корпоративной мобильностью, компания реализовала концепцию BYOD для более чем 20 000 сотрудников и мобилизовала сотни разноплатформенных приложений.

Организации здравоохранения внедряют концепцию BYOD, чтобы врачи и медицинские работники могли приносить собственные устройства и работать с ними в любом месте и в любое время, например, просматривать медицинские карты пациентов на планшете во время обхода, просматривать контрольные данные в реальном времени на смартфоне во время поездок или дистанционно участвовать в онлайн-консультации. Соответствие данного решения нормативным требованиям обеспечивается за счет соответствующего уровня доступа к данным и приложениям согласно сценариям, а также защиты и возможности удаленной блокировки или удаления всех клинических данных и информации о пациентах.

Компания розничной торговли, владеющая 70 супермаркетами, использовала XenMobile, чтобы организовать доставку ИТ-услуг в свои торговые точки согласно концепции BYOD, централизовать обслуживание и управлять ИТ-расходами. Решение Citrix позволяет предоставлять дифференцированные услуги в зависимости от расположения: небольшие магазины франчайзи, получают базовые SaaS-приложения, например Google Apps®, а крупные сетевые магазины получают высокотехнологичные облачные приложения, например Microsoft Office® 365. Кроме того, все магазины получают корпоративный стандартный пакет программных средств для кассовых терминалов. Пользователи могут получить доступ к своим приложениям с любого устройства, включая личные устройства потребительского класса.

Транспортная логистическая компания использует XenMobile, чтобы реализовать безопасную концепцию BYOD для сторонних подрядчиков и 15 000 своих партнеров, предоставляя при этом услуги, дифференцируемые в зависимости от партнера и географии. Клиенты из нефтегазовой отрасли активно развивают «родные» мобильные приложения и внедряют мобильные устройства для использования работниками «в поле». По отзыву одной из компаний, «унифицированный магазин приложений является, на наш взгляд, единственным решением для эффективной доставки новых мобильных приложений, а также корпоративных веб-приложений, виртуальных приложений и приложений SaaS».

Предприятия в сфере **транспорта** используют XenMobile для мобилизации операторов сборочной линии и создания безопасной среды обмена для поставщиков. Теперь внутренние и сторонние пользователи имеют доступ к приложениям в унифицированной среде, охватывающей всю цепочку создания стоимости, куда включены импортные поставки, операции, внешняя логистика, маркетинг, продажи и поставки.

Клиенты из сферы **телекоммуникаций** создают новые платные услуги по доставке мобильных приложений и данных в соответствии со своим бизнесом по продаже мобильных устройств и предоставления услуг голосовой связи и передачи данных.

Клиенты, представляющие различные отрасли и сферы деятельности, от **средств массовой информации и развлечений** до **строительства**, также используют XenMobile для мобилизации данных, что служит ярким примером необходимости внедрения средств управления корпоративной мобильностью в организациях любых типов и уникальной эффективности решения Citrix в реализации этой стратегии.

Вывод

BYOD – не просто тенденция. Это значимая новая модель, позволяющая сотрудникам выбирать наилучший способ работы и обеспечивающая полную мобильность и производительность на предпочитаемом устройстве. Для нового мобильного предприятия управление устройствами является лишь одним из элементов комплексной стратегии. MDM-решения должны быть дополнены более полноценными возможностями доставки, обеспечения безопасности и контроля всего спектра приложений, необходимых для работы. Теперь, используя комплексное решение для корпоративной

мобильности Citrix XenMobile, ИТ-отделы могут легко управлять постоянно растущим числом разнообразных мобильных устройств и платформ и увеличивать приносимую ими пользу, сосредоточив внимание на управлении бизнесконтентом. Благодаря этому простому, но всеобъемлющему подходу ИТ-службы могут реализовать свои стандарты безопасности и управления, одновременно обеспечивая пользователям полную свободу выбора и более удобную, продуктивную среду для работы. Предоставляя наиболее полный и ориентированный на пользователя подход к мобильности в отрасли, а также средства безопасного обмена файлами и организации совместной работы, Citrix помогает компаниям в различных сферах деятельности и странах мира реализовать весь потенциал BYOD.

Дополнительные ресурсы

Веб-сайт: www.citrix.com/xenmobile

Техническое описание: 10 обязательных условий для безопасности мобильных средств предприятия

Техническое описание: Как сделать предприятие мобильным: контрольный список руководителя

Представительство Citrix Systems в России и странах СНГ

Комплекс Москва Сити, Северная башня
Адрес: 123317, г. Москва,
ул.Тестовская д.10, Тел.
+7 495 662 1726
www.citrix.com

О Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) – компания, которая в эру «облачных» технологий трансформирует индивидуальную и совместную работу бизнеса и ИТ. Предлагая ведущие на рынке «облачные», сетевые и виртуализационные технологии, Citrix открывает новые возможности в области мобильной работы и предоставления «облачных» услуг, существенно

упрощая и делая более доступными сложные ИТ-процессы для более чем 260 000 предприятий. Каждый день Citrix соприкасается с 75% пользователей Internet и работает с более чем 10 000 компаний в 100 странах мира. Годовая выручка в 2012 году составил 2,59 миллиарда долларов США. Узнать больше на сайте www.citrix.com.

0413/PDF