Взгляд Dell на ключевой тренд – консьюмеризация ИТ

За все время существования ИТ как индустрии начиная с 50-х годов прошлого века произошло несколько важных и революционных изменений в этой сфере. Одним их таких прорывных достижений является появление мобильных технологий и их экспансивное распространение на все сферы деятельности людей, в том числе появление тенденции использования сотрудниками компаний своих личных устройств для выполнения бизнес-задач.

В самом деле, кто не предпочтет работать на собственном ноутбуке или планшете, который человек так тщательно выбирал с учетом своих индивидуальных требований, вместо унифицированного, часто неудобного устройства, выданного организацией? К тому же, если сотруднику привычнее общаться с клиентами в социальных сетях либо хранить материал на SkyDrive, разве он не найдет способ использовать для работы именно эти ресурсы вместо авторизованных ИТ-отделом аналогов?

Таким образом, тенденция, получившая название "консьюмеризация ИТ", т.е. проникновение технологий из потребительской среды в корпоративную, просто не могла не зародиться. И в ближайшие годы она будет только усиливаться. По оценкам компании Forrester, к 2015 году 90 % прироста продаж компьютерной техники придется на смартфоны и планшеты, и при этом 50 % мобильных устройств, используемых в организациях, будут находиться в фактической собственности сотрудников. Распространение мобильных технологий и средств связи в корпоративной среде кардинально меняет способ организации рабочего процесса и взаимодействия персонала с партнерами и коллегами. И вопрос, который встает перед ИТ-отделами, уже заключается не в том, как предотвратить использование несанкционированных устройств в корпоративной сети, а в том, как адаптировать ИТ-инфраструктуру компании, чтобы дать сотрудникам возможность продуктивно работать в любое время, в любом месте и с помощью удобных для них устройств, при этом обеспечив достаточный уровень безопасности данных.

Ответом на этот вопрос является проактивное внедрение концепции BYOD ("принеси свое устройство"), т.е. обеспечение для работающего персонала доступа к корпоративной сети и ресурсам компании с личных устройств. Важен именно проактивный подход, так как промедление или игнорирование проблемы может создать дополнительные риски для организации. Согласно упомянутому исследованию Forrester, уже сейчас треть сотрудников пытается использовать несанкционированные личные устройства в своей работе, и при этом 37 % из них считают, что обеспечение безопасности корпоративных данных является задачей исключительно ИТ-отдела, а не самих сотрудников.

Безусловно, целесообразность и степень реализации BYOD будут индивидуальны для каждой организации в зависимости от ее бизнес-стратегии. Очевидно, что проект BYOD связан с большим комплексом работ, с дополнительными инвестициями в ИТ и с риском потери или кражи конфиденциальных данных. Однако при правильном его исполнении в тесном сотрудничестве ИТ-специалистов с персоналом бизнес-подразделений полученные преимущества окажутся более весомыми. Среди таких преимуществ можно назвать следующие:

- повышенная гибкость и продуктивность сотрудников, их более эффективная кооперация и коммуникация между собой и с клиентами;
- возможность использовать новейшие устройства и технологии для работы, не дожидаясь обновления корпоративного парка компьютеров;
- высвобождение времени ИТ-персонала благодаря автоматизации управления клиентскими устройствами;
- повышенная безопасность корпоративной сети и данных после внедрения специальных решений;
- экономия затрат на офисные помещения за счет перевода части сотрудников в режим удаленной работы.

Подход к реализации проекта BYOD можно разделить на четыре основных этапа:

1. ***Утверждение стратегии.***
   На этом этапе следует:
   - определить, деятельность каких сфер организации может действительно получить положительный эффект от внедрения BYOD;
   - оценить существующую ИТ-инфраструктуру и возможность ее масштабирования;
   - рассчитать допустимый уровень риска для корпоративной сети и данных, связанных с использованием личных устройств.
2. ***Определение политик.***
   Здесь требуется ответить на ряд вопросов:
   - какие типы устройств и операционных систем следует разрешить к использованию;
   - к каким корпоративным ресурсам и приложениям нужно обеспечить доступ с личных устройств;
   - сотрудникам какого уровня и каких подразделений дозволяется доступ к корпоративным ресурсам и приложениям;
   - как обеспечивать безопасность коммерческих данных и корпоративной сети;
   - как осуществлять техническую поддержку личных устройств;
   - будет ли и в какой степени компенсироваться стоимость устройства сотруднику.
3. ***Выбор средств обеспечения защиты.***
   Защита должна строиться с учетом трех ее уровней:
   - средства, интегрированные в устройства;
   - защита канала передачи данных;
   - система выявления рисков и предотвращения угроз.
4. ***Обеспечение максимальных возможностей для сотрудников.***
   Нужно, в частности, проанализировать:
   - требуется ли модернизация бизнес-приложений для современных интерфейсов различных платформ;
   - могут ли бизнес-приложения работать в виртуальной среде;
   - следует ли перевести сотрудников на корпоративный контракт с поставщиком услуг беспроводной связи.

Успех проекта BYOD во многом зависит от партнера-поставщика, предлагающего большой выбор решений и экспертизу в данной области. На сегодняшний день на рынке существует масса предложений ПО и услуг от разных компаний, но проблема заключается в том, что по большей части все это специализированные решения, ориентированные на какую-то конкретную задачу – удаленное управление устройствами, обеспечение безопасности данных, модернизация приложений или оптимизация инфраструктуры. Разобраться во всех нюансах предлагаемых продуктов и совместить их в единое комплексное решение – непростая задача.

В свою очередь, компания Dell сформировала большой портфель ПО и услуг для BYOD и является, пожалуй, единственным поставщиком полного спектра законченных BYOD-решений – от серверного оборудования до программного обеспечения и клиентских устройств. По сути, любой заказчик может "в режиме одного окна" подобрать среди предложений Dell именно то решение, которое подойдет для данной конкретной организации, и получить необходимую экспертизу по развертыванию BYOD-проекта и управлению им.

Возьмем для примера задачу удаленного управления мобильными устройствами (MDM). Здесь Dell предлагает два варианта:

1. ***Dell Wyse Cloud Client Manager*** – облачное решение как услуга (SaaS), позволяющее проводить инвентаризацию, создавать групповые политики, вести мониторинг использования оборудования. Кроме поддержки мобильных устройств на iOS и Android оно позволяет также управлять стационарными тонкими клиентами и ПК, т.е. является единым решением для управления всем парком устройств в компании.

2. ***Dell KACE 3000*** – программно-аппаратный комплекс, который интегрируется в серверную стойку и позволяет решать такие задачи, как инвентаризация, управление устройствами, приложениями и профилями, создание групповых политик, обеспечение безопасности данных на устройстве и т. д. Решение поддерживает все современные платформы (iOS, Windows, Android) и легко масштабируется путем приобретения дополнительных лицензий.

Но даже MDM-решение не гарантирует полной безопасности передачи данных. На большинстве потребительских устройств данные не шифруются на аппаратном уровне. Лучший способ обеспечить их конфиденциальность – внедрить средства защиты как на устройстве, так и на уровне сети и в дата-центре. Для двух последних задач оптимально подойдут продукты Dell SonicWall SSL VPN и межсетевые экраны Dell SonicWall FireWall.

Как уже упоминалось, BYOD только тогда будет иметь ценность, когда реализация проекта приведет к повышению эффективности персонала, процессов и систем. В 60 % случаев это напрямую зависит от наличия удаленного доступа сотрудников к критически важным бизнес-приложениям с личных устройств. Но разработка приложений или адаптация их к новым интерфейсам может оказаться затратным мероприятием как по стоимости, так и по времени. Решения Dell по виртуализации рабочего стола позволят гораздо быстрее обеспечить доступ сотрудников к корпоративным приложениям с любых ПК. При этом, постоянно работая с Citrix, VMware и другими производителями программного обеспечения над "бесшовной" совместимостью их ПО с оборудованием Dell, компания обладает исключительной экспертизой в развертывании таких решений – вплоть до оптимизации сетевой инфраструктуры с таким уровнем исполнения, когда разница в работе с виртуальным и обычным рабочим столом для пользователя полностью исчезает. Кроме того, решения по виртуализации обладают массой преимуществ с точки зрения безопасности данных, так как информация не попадает на само клиентское устройство. Если же в этом случае требуется увеличение пропускной способности сетевой инфраструктуры, сетевые решения Dell окажутся в два раза экономичнее многих конкурентных предложений.

Потребительские устройства привлекают пользователей дизайном, модностью, множеством доступных приложений, но при этом представляют определенную сложность для интеграции в ИТ-инфраструктуру. В некоторых случаях затраты на внедрение BYOD можно сократить, ограничив выбор для сотрудников набором заранее авторизованных устройств. Для такого сценария Dell разработала целую линейку продуктов XPS, которые, с одной стороны, обладают всеми преимуществами потребительских устройств, а с другой – предусматривают возможность использования сервисов корпоративного класса: загрузка корпоративного образа и настройки BIOS в соответствии с требованиями заказчика при производстве, круглосуточная техническая поддержка и выезд специалиста к клиенту для диагностики и ремонта оборудования. Все ноутбуки, ультрабуки и планшеты Dell XPS используют Windows ОС, что позволяет легче интегрировать их в уже существующую инфраструктуру на технологиях Microsoft.

Консьюмеризация ИТ происходит, и происходит она вне зависимости от того, хотим мы этого или нет. Высокоскоростные коммуникационные технологии и развитие рынка мобильных устройств кардинально меняют ожидания сотрудников от ИТ-служб и стирают границу между работой и личным временем, между корпоративным и собственным оборудованием. Неуправляемый процесс подвергает организации новым рискам: 50 % ИТ-менеджеров уже в той или иной степени сталкивались с нарушением политик при использовании личных устройств. Задача руководителей организаций и ИТ-директоров – не создать сотрудникам преграду, а использовать эту тенденцию для повышения эффективности и продуктивности бизнеса. По подсчетам, персонал, использующий мобильные устройства, работает в среднем на 240 часов в год больше, чем остальные сотрудники. А экономия на общей стоимости владения при использовании личных устройств, по оценкам Gartner, может составить от 9 до 43 %. Таким образом, задача создания условий для максимального использования потенциала сотрудников, по сути, становится ответом на вопрос, получит ли ваша компания дополнительное конкурентное преимущество на рынке.

Денис Минов, менеджер по маркетингу потребительского направления, компания Dell

ПЕРЕДОВЫЕ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ

ПТА

ВЫСТАВКА

XIII Международная специализированная выставка

Передовые Технологии Автоматизации

ПТА-2013

8-10 октября

Москва, ЦВК «Экспоцентр», павильон 5

Тематика выставки:

- Автоматизация промышленного предприятия
- Автоматизация технологических процессов
- Системная интеграция и консалтинг
- Автоматизация зданий
- Бортовые и встраиваемые системы
- Электротехника. Электроэнергетика NEW

При поддержке:

Организатор:

Экспоцентр

Москва:
Тел.: (495) 234-22-10
E-mail: info@pta-expo.ru

www.pta-expo.ru

16+