КРАТКИЙ ОБЗОР

CIO Strategic Marketing Services

Модернизация процессов управления и обеспечения безопасности Windows 10 с помощью решения VMware AirWatch для централизованного управления конечными устройствами

Развитие потребностей сотрудников

СЕГОДНЯ СОТРУДНИКИ как никогда мобильны и независимы. Использование мобильных устройств для работы становится все более популярным, и персонал полагается на множество приложений, устройств и облачных услуг. Многие сотрудники используют одно устройство как для корпоративных, так и для личных задач, и ожидают гибкие условия работы, конфиденциальность и поддержку самообслуживания. Если ИТ-среда не будет соответствовать этим ожиданиям, будет сложно избежать разочарования сотрудников, которые в отсутствие удобных условий работы станут более активно использовать «теневые» ИТ-услуги.

Кроме того, и работа самого ИТ-отдела является в значительной степени разрозненной: одни группы управления отвечают за настольные компьютеры, а другие — за мобильные устройства. Для администрирования мобильных устройств используются современные решения по управлению корпоративной мобильной средой (enterprise mobility management, EMM). Однако управление настольными компьютерами до сих пор осуществлялось отдельно с использованием традиционных средств управления жизненным циклом ПК (PC lifecycle management, PCLM).

Такая фрагментированная модель управления не соответствует ожидаемому уровню расходов и безопасности. Так как пользователи больше не привязаны к офисам, а для работы традиционных средств PCLM устройства должны быть присоединены к корпоративному домену и сети для получения ИТ-политик и обновлений ОС, возрастают риск несоответствия требованиям и количество возможных типов атак.

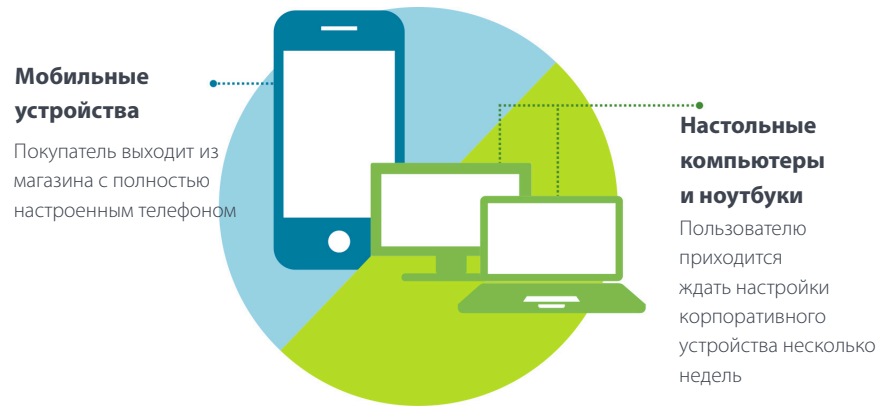
Для соответствия потребностям современного мобильного персонала сначала необходимо устранить разрозненность групп управления и реализовать согласованный, ориентированный на пользователя подход к управлению всеми конечными устройствами. По мнению аналитика Gartner Криса Сильвера (Chris Silver), «будущее управления конечными устройствами заключается в консолидации средств управления традиционными ПК и мобильными устройствами в рамках эволюционирующего единого подхода».

Благодаря реализации протоколов управления мобильными устройствами в Windows 10 ИТ-отделы получили возможность объединить разные группы управления ИТ-ресурсами, консолидировать средства управления, снизить расходы, повысить эффективность ИТ-инфраструктуры и уровень корпоративной безопасности. Теперь организации могут упростить управление пользовательскими устройствами путем использования централизованного решения по управлению конечными устройствами (unified endpoint management, UEM) для администрирования как настольных компьютеров, так и мобильных устройств.

ОГРАНИЧЕНИЯ ТРАДИЦИОННОГО ПОДХОДА К УПРАВЛЕНИЮ ПК

Основной целью ИТ-отдела должно быть создание удобной рабочей среды для конечных пользователей, в которой они смогут работать более эффективно. Однако условия работы пользователей на мобильных устройствах и ПК во многом противоположны. Развертывание и настройка мобильных устройств могут быть эффективно выполнены пользователями в режиме самообслуживания. Для развертывания настольного компьютера или ноутбука требуется множество часов, которые уйдут на подготовку образов, настройку и обслуживание.

Пользователи все больше недовольны тем, что настройка ПК является медленным и неудобным процессом по сравнению с настройкой и администрированием мобильных устройств.



Что необходимо изменить?

1 Операционная система

Операционная система Windows — это первый элемент, который должен развиваться с учетом потребностей сотрудников. Windows 10 представляет собой ориентированную на потребителя ОС с возможностями персонализации, обеспечения конфиденциальности и мобильности. Кроме того, в этой версии Windows предложен принципиально новый подход к защите и управлению ОС, согласованный с современными EMM-решениями. Единый набор протоколов управления на ПК, планшетах и телефонах с операционной системой Windows 10 поможет ИТ-отделам консолидировать средства управления, быстро инициализировать устройства, а также передавать политики и приложения по сети, чтобы пользователи могли в кратчайшее время приступить к работе.

2 Средства управления

Традиционные средства управления ПК не соответствуют требованиям сотрудников, которым необходима возможность работать в любой точке, в любое время и на любом устройстве. Пользователям требуются согласованные процессы доступа к рабочим приложениям и данным на всех устройствах. ИТ-отделам, которые продолжают использовать традиционные средства для управления ПК, становится все сложнее соответствовать этим ожиданиям по следующим причинам.

- Высокая стоимость. Традиционные подходы к управлению ПК трудоемки и характеризуются значительным объемом серверных ресурсов, множеством программных решений и сложностью создания образов и управления конфигурацией. Управление программными пакетами и исправлениями ОС — это трудоемкий процесс; при этом ИТ-отделу необходимо развивать и сохранять имеющиеся навыки управления как настольными компьютерами, так и мобильными устройствами.

- **Низкий уровень безопасности.** Управление чаще всего осуществляется с помощью объектов групповой политики, которые доступны только для устройств, присоединенных к сети и домену. При использовании такого подхода для полного внедрения политик безопасности и установки исправлений ОС и обновлений приложений может потребоваться несколько недель или даже месяцев, при этом повышаются риски нарушения безопасности в организации. По мере появления новых типов атак ИТ-специалистам становится все сложнее получить необходимый уровень визуализации работоспособности конечных устройств и их соответствия нормативным требованиям.

- **Ограниченные возможности.** Традиционные подходы ограничивают контроль пользователей над устройствами. Для повышения уровня безопасности ИТ-отделам необходимо ограничить типы используемых устройств и разрешить установку только проверенных приложений и обновлений в ОС. В результате возможности персонализации ограничены, а для пользователей не поддерживается режим самообслуживания. Подобные ограничения приводят к росту числа обращений в службу ИТ-поддержки даже по несложным вопросам, таким как установка приложения на устройстве.

НАСТУПЛЕНИЕ ЭПОХИ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ КОНЕЧНЫМИ УСТРОЙСТВАМИ

Появление API-интерфейсов управления мобильными устройствами в Windows 10 кардинально меняет возможности управления ПК в организациях. Однако с персональными компьютерами, в отличие от iOS и Android, связано несколько уникальных задач.

- Необходимость в поддержке сложных сценариев и объектов групповой политики.
- Инкапсуляция и распространение классических приложений Windows (Win32).
- Тестирование исправлений ОС перед их предоставлением пользователям.
- Объем передаваемых приложений и обновлений приводит к перегрузке сети.

Организациям необходима централизованная платформа управления конечными устройствами, которая предоставит эффективную рабочую среду для ИТ-отдела и конечных пользователей, аналогичную возможностям EMM-решений для мобильных устройств, в сочетании с гибкими возможностями управления, доступными в традиционных средствах управления ПК.

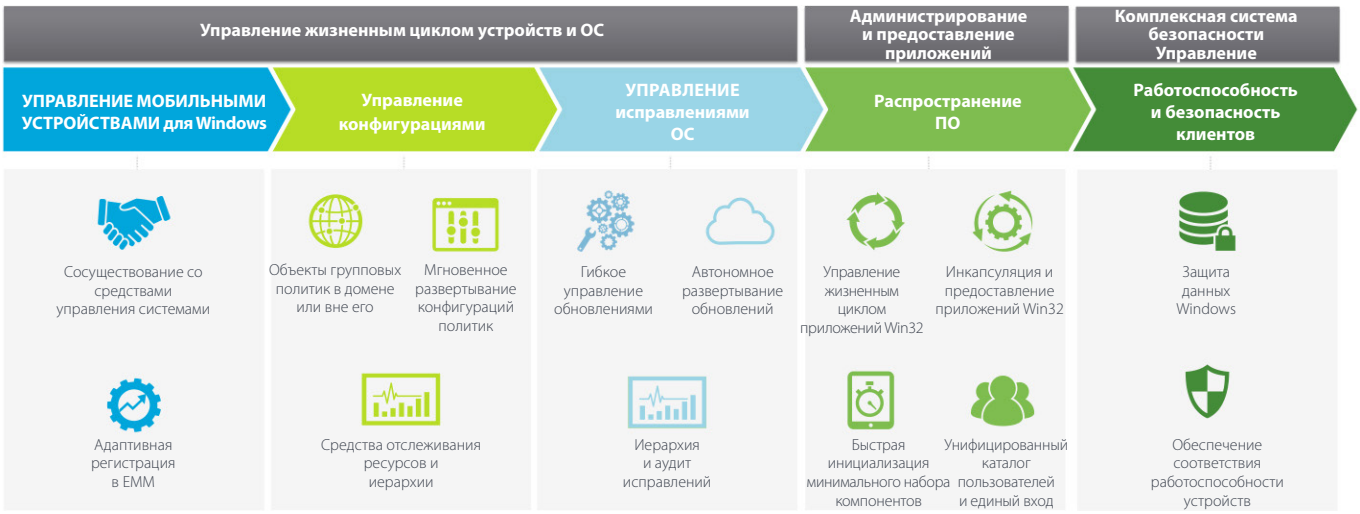
В решении VMware AirWatch Unified Endpoint Management для централизованного управления конечными устройствами реализован полный набор возможностей Windows 10 для развертывания и настройки ОС, распространения приложений (в том числе Win32) и обновлений, а также для обеспечения комплексной защиты. Благодаря современному подходу, ориентированному на облако, это решение сокращает расходы и нагрузку на ИТ-отдел, а также предоставляет удобные и безопасные механизмы управления Windows 10. Теперь ИТ-отделы получают возможность решить следующие задачи.

- Переход от трудоемкого процесса создания образов к более удобной модели развертывания.
- Реализация распространения исправлений ОС и программного обеспечения для устройств вне домена и в любой сети.
- Инициализация самостоятельного доступа для пользователей и широкий выбор возможностей, устройств и приложений.
- Поддержка совместного размещения личных и рабочих данных на устройствах.
- Поддержка мгновенной визуализации, безопасности и соответствия нормативным требованиям для всех конечных устройств в сети и вне ее.

Благодаря платформе AirWatch UEM возможности управления Windows можно масштабировать для любого сценария использования.

- Развертывание Windows 10 для удаленных пользователей.
- Подключение личных устройств сотрудников.
- Реализация корпоративных развертываний в филиалах.
- Управление специальными терминалами бизнес-подразделений.

AirWatch UEM предоставляет более удобные, безопасные и экономичные возможности управления устройствами



РАЗВЕРТЫВАНИЕ ОРИЕНТИРОВАННЫХ НА ОБЛАКО СРЕДСТВ УПРАВЛЕНИЯ И БЕЗОПАСНОСТИ В ОС WINDOWS

Управление мобильными устройствами для Windows

AirWatch поддерживает единые рабочие процессы регистрации различных устройств: корпоративных и личных, присоединенных к домену, новых или уже используемых. AirWatch помогает преобразовать обычное OEM-устройство в проверенное и готовое к использованию без необходимости в создании образов, что экономит время и денежные средства. В дополнение к рабочим процессам, выполняемым ИТ-отделом, AirWatch предоставляет конечным пользователям возможности для самостоятельной регистрации устройств.

Кроме того, для пользователей с личными устройствами и подрядчиков в AirWatch реализована пошаговая регистрация в системе управления, учитывающая уровень конфиденциальности приложений и требования безопасности. Например, доступ к базовым офисным приложениям может быть предоставлен с помощью специализированного каталога приложений компании на основе учетных данных и прав пользователя. Однако доступ к приложениям, которые содержат конфиденциальные корпоративные данные, предоставляется только в том случае, когда устройство полностью контролируется AirWatch.

С помощью этой современной платформы управления облаком и мобильностью AirWatch может управлять зарегистрированными устройствами с ОС Windows, а также быстро развертывать политики на устройствах по сети. С каждым обновлением Windows 10 корпорация Microsoft расширяет набор протоколов управления, доступных поставщикам EMM-решений. Благодаря этому возможности управления профилями пользователей и параметров все больше похожи на возможности, доступные для мобильных устройств. Например, использование паролей, настройка электронной почты, активация корпоративного доступа к сетям Wi-Fi и VPN, а также задание ограничений для устройств и приложений направлены на упрощение настройки ОС и повышение уровня безопасности.

Управление конфигурациями

При управлении ПК с Windows ИТ-отдел часто использует сложные процедуры автоматизации, состоящие из сложных сценариев, политик объектов групповой политики и других традиционных параметров управления ПК. Например, компаниям может требоваться специальный фон рабочего стола для их компьютеров, а также возможность удалить избыточное программное обеспечение и выполнить специализированную настройку политик брандмауэра и антивирусного ПО. Благодаря возможностям AirWatch для управления конфигурацией ИТ-отдел может создавать «продукты», включающие в себя эти файлы, приложения или параметры. Такие продукты можно мгновенно развертывать на устройствах по сети; их также можно связать с более сложной последовательностью процедур и условиями установки.

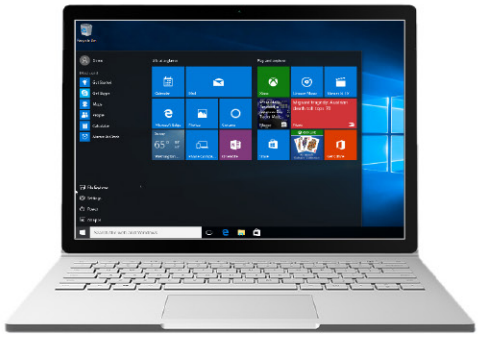
Управление исправлениями ОС

Поскольку центр обновления Windows предоставляется как услуга, корпорация Microsoft передает накопительные обновления ОС по сети. Обновления, которые прошли серьезный цикл тестирования, предоставляются как готовые к использованию в корпоративной среде. Несмотря на то что предоставление и обслуживание на базе облака дают определенные преимущества, ИТ-специалисты по-прежнему боятся потерять контроль над следующими элементами.

- Типы распространяемых обновлений
- Возможное нарушение работы ОС из-за отсутствия тщательного тестирования обновлений в компании
- Перегрузка сети, поскольку размер обновлений может достигать нескольких гигабайт

Используя AirWatch, ИТ-отделы могут развертывать и (или) откладывать обновления и исправления ОС с учетом приоритета устройств и планируемых окон обслуживания. ИТ-специалисты получают возможность

Wi-Fi | VPN | Сертификаты | Эл. почта | Пароли | Соответствие нормативам ограничения | Шифрование | Брандмауэр и антивирус | Управление лицензиями на ОС



AirWatch упрощает настройку и администрирование устройств по сети.

задать автоматическое утверждение обновлений для некоторых групп (например, для приложений, разработчиков, безопасности и т. д.) или исключить такие группы в зависимости от важности обновлений компонентов и системы безопасности для конкретных пользователей. Благодаря одноранговому кэшированию AirWatch оптимизирует предоставление обновлений и предотвращает перегрузку сети. ИТ-специалисты могут получать подробные сведения о иерархии и проводить аудит соответствия отдельных обновлений Windows нормативным требованиям, а также устранять сложности, связанные с автономной установкой исправлений.

Распространение ПО

Благодаря универсальной платформе Windows (Universal Windows Platform, UWP) корпорация Microsoft унифицировала работу приложений на всех устройствах под управлением Windows 10. Общедоступные приложения UWP теперь могут предоставляться из Windows Store, аналогичного другим магазинам для различных мобильных ОС, или с использованием внутреннего корпоративного магазина, настроенного для организации. Интеграция AirWatch с Windows Store и Windows Store for Business оптимизирует предоставление современных приложений.

Однако большинство корпоративных программных продуктов для Windows представляют собой классические приложения Win32, занимающие большой объем на диске и сложные в инкапсуляции, развертывании и обслуживании. По этой причине распространение ПО становится одной из самых сложных задач при управлении Windows с использованием EMM-решений. AirWatch справляется с этой задачей, устраняя расхождения между управлением жизненным циклом приложений UWP и Win32.

Используя AirWatch, ИТ-специалисты могут консолидировать управление мобильными приложениями и традиционные возможности развертывания программного обеспечения Win32 в единой консоли администрирования. Благодаря этому администраторы могут управлять исправлениями сторонних приложений, развертывать зависимые компоненты и даже настраивать условия установки приложений.

С помощью AppStacks платформа AirWatch реализует новый подход к предоставлению ПО, устраняющий проблемы инкапсуляции и ненадежности установки приложений. ИТ-отдел сможет быстрее развертывать приложения Win32 на всех устройствах под управлением Windows с уровнем удобства и надежности, аналогичным развертыванию мобильных приложений. Конечным пользователям AirWatch предоставляет каталог самообслуживания и согласованные возможности единого входа для всех приложений Windows — в том числе стандартных, предоставляемых по модели «ПО как услуга» и удаленных приложений.

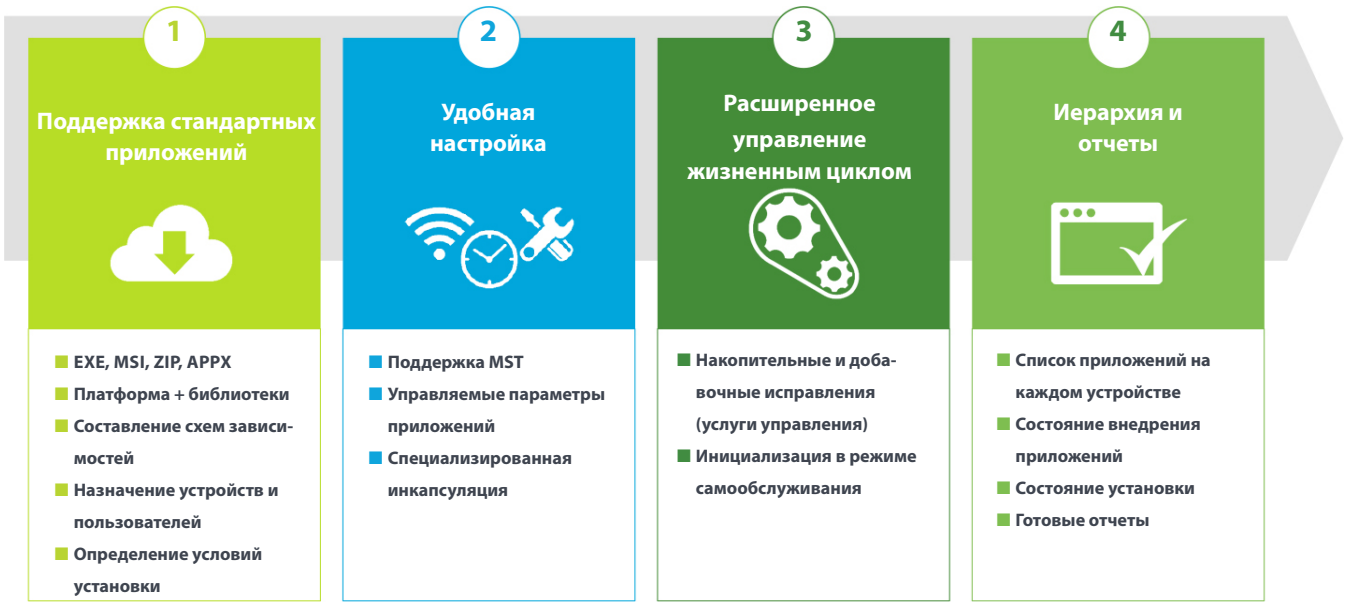
Работоспособность и безопасность клиентов

Для решения современных задач кибербезопасности также требуется комплексная система защиты. AirWatch устанавливает отношения доверия с пользователями, улучшает защиту ОС от новых угроз и обеспечивает разделение рабочих и персональных данных для защиты хранимых, используемых и передаваемых корпоративных данных.

Доверие пользователей.

Даже самые надежные пароли являются уязвимыми, так как их можно украсть многими способами, например с помощью фишинговых атак, вредоносных программ и перехвата нажатия клавиш. Интеграция AirWatch с возможностями управления учетными данными

Возможности управление приложениями Win32



Windows 10 обеспечивает поддержку политик проверки подлинности без пароля с использованием жестов или ПИН-кода. Организации могут без дополнительной настройки включить многоуровневую проверку подлинности для защиты от атак типа «передача хэша».

Эффективная защита ОС. С помощью AirWatch ИТ-специалисты могут принимать профилактические меры защиты для предотвращения скачивания или выполнения ненадежных или неутвержденных приложений. AirWatch проверяет целостность устройств и их соответствие нормативным требованиям в режиме реального времени и автоматически блокирует доступ несоответствующих устройств к корпоративным приложениям и службам.

Защита данных. Предотвращение потерь данных является для организаций первоочередной задачей, поскольку устройства становятся все более мобильными, что повышает вероятность их кражи или потери. Кроме того, пользователи часто используют одно устройство для выполнения как рабочих, так и личных задач. AirWatch реализует политики шифрования данных, предоставляет администраторам и конечным пользователям возможности удаленной очистки в случае кражи или потери устройства, а также обеспечивает разделение рабочих и личных данных, используя встроенные возможности контейнеров ОС Windows.

AirWatch UEM помогает организациям без лишних расходов реализовать возможности комплексного управления безопасностью.

ЗАЩИТА ВСЕХ КОНЕЧНЫХ УСТРОЙСТВ НА БАЗЕ ЕДИНОЙ ПЛАТФОРМЫ

Система UEM должна быть не зависящим от платформы единым решением для управления каждым устройством и операционной системой в любом сценарии использования в организации. Такой подход обеспечивает единообразные условия работы конечных пользователей вне зависимости от того, какие устройства они используют для доступа к корпоративной среде.

AirWatch UEM предоставляет целостный, ориентированный на пользователей подход к администрированию и защите любого конечного устройства на базе единой платформы. Это решение поддерживает глобальное развертывание в различных подразделениях и регионах с использованием единой консоли на базе архитектуры с поддержкой нескольких арендаторов. Интеграция AirWatch UEM с корпоративными системами помогает извлечь максимальную пользу из инвестиций в инфраструктуру и использовать имеющиеся службы для всех конечных устройств.

Благодаря VMware AirWatch UEM ИТ-специалисты могут автоматизировать процессы с помощью динамических и интеллектуальных модулей политик на платформах Windows 10. Это помогает устранить выполняемые вручную ИТ-задачи и предоставить пользователям возможности самообслуживания, что сокращает расходы на поддержку.

Вы готовы по-новому взглянуть на управление конечными устройствами? Мы предлагаем вам воспользоваться бесплатной 30-дневной пробной версией и зарегистрировать до 100 устройств. Дополнительные сведения см. на веб-сайте.