Передовые методы простого и безопасного управления устройствами

Мобильная производительность для вашего бизнеса.
Свобода выбора для сотрудников.
Полная безопасность и контроль для ИТ-отдела.

Современная ИТ-стратегия ориентирована на предпочтения сотрудников. Предоставляя сотрудникам возможность выбирать лучшие устройства, удовлетворяющие их потребностям, организации могут повысить производительность, гибкость и даже уровень удовлетворенности работой. С помощью правильной стратегии ИТ-отдел может обеспечить применение надлежащих политик и технологий для защиты бизнес-информации, в то же время снижая расходы и обеспечивая высокую комфортность работы пользователей.

Ваша стратегия должна гарантировать вашей организации следующее:

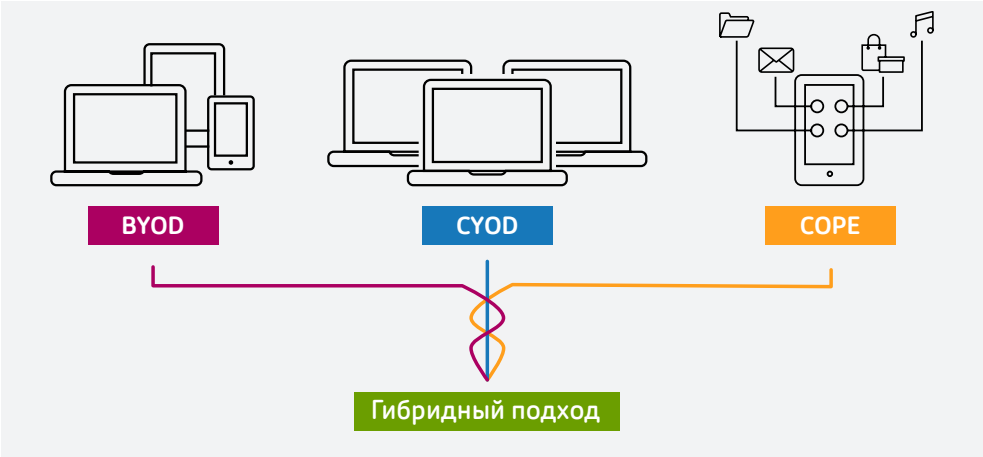
- **предоставление сотрудникам возможности** выбирать собственные устройства для улучшения их производительности, совместной работы и мобильности;
- **обеспечение защиты секретной информации** от утери и хищения с соблюдением конфиденциальности, требований регулирующих органов и стандартов управления рисками;
- **снижение затрат и упрощение управления** путем введения самостоятельного провижининга, автоматизированного управления и мониторинга;
- **упрощение ИТ-инфраструктуры** за счет единого комплексного решения для управления и защиты данных, приложений и устройств.

Ниже представлены 8 передовых методов разработки стратегии, сочетающей простоту для сотрудников с эффективностью обеспечения безопасности, контроля и управления для ИТ-отдела.

1. Выбор политики

По мере того как мобильность и ориентация на потребителя продолжают трансформировать сферу ИТ, появился ряд политик, которые сочетают в себе свободу выбора и повышенный контроль со стороны ИТ-отдела.

- Концепция BYOD (использование собственных устройств): дает сотрудникам возможность использовать для работы личные устройства.
- Концепция CYOD (использование устройства по своему выбору): дает сотрудникам возможность выбирать из небольшого числа принадлежащих компании устройств для использования в рабочих целях.
- Концепция COPE (использование корпоративных устройств, которые сотрудник настраивает и обслуживает самостоятельно): дает сотрудникам возможность выбирать принадлежащее компании устройство из одобренного списка и использовать на нем собственные и корпоративные приложения.
- Гибридный подход: чтобы обеспечить мобильность для разных пользователей и групп, можно использовать сочетание этих вариантов. Например, концепцию COPE можно использовать наряду с CYOD или BYOD.



Несмотря на то что нюансы политик могут отличаться, в каждой применяются фундаментальные принципы унифицированного управления конечными устройствами (UEM), включая факторы, связанные с обеспечением безопасности. Основные отличия связаны с затратами.

Пользователи BYOD платят за собственные устройства и тарифные планы, иногда с частичной или полной компенсацией расходов со стороны компании. В случае COPE и CYOD использование устройств и данных оплачивает компания. В рамках политики BYOD также необходимо учитывать вопросы, выходящие за рамки COPE и CYOD, например вопрос о том, следует ли платить сотрудникам за сверхурочную работу, если они проверяют электронную почту в нерабочее время или по выходным.

2. Предоставление права и регистрация

Вы должны четко обозначить, кому из сотрудников разрешено использовать личные устройства либо на нерегулярной основе в дополнение к корпоративному конечному устройству, либо для постоянного замещения корпоративного устройства, либо в качестве промежуточного варианта. Это может рассматриваться как привилегия, которую нужно заслужить, как удовлетворение потребностей сотрудников, как необходимое требование для определенных типов должностей, как избыточный риск в некоторых случаях или, чаще всего, как сочетание указанных вариантов.

Определять, кто обладает правом на участие в программе такого рода, можно, например, по таким критериям, как тип должности, частота командировок, эффективность сотрудника и необходимость в автономном доступе к конфиденциальным данным. Несмотря на то что предоставление этого права определяется на основе самых разных факторов, за руководителями должно всегда оставаться последнее слово в утверждении сотрудников, которые могут стать кандидатами на получение субсидии. Руководителям также рекомендуется применять подходы BYOD, COPE и CYOD в контексте других служебных поощрений, привилегий и дисциплинарных мер.

Как правило, для программы BYOD самыми подходящими кандидатами являются подрядчики. В большинстве организаций от подрядчиков уже ожидают использования собственных устройств, и это требование нацелено на обеспечение соответствия независимых подрядчиков стандартам.

3. Разрешенные устройства

Во избежание появления трудно поддающегося контролю многообразия устройств ваша компания может ограничить тип поддерживаемых мобильных устройств. Детальность данной политики будет зависеть от ваших требований к пользователям, связанных с безопасностью рисков и ресурсов поддержки. В целом, чем более детальна ваша политика в отношении типов устройств, версий ОС и номеров моделей, тем больше ресурсов вам потребуется для надлежащего тестирования и поддержки указанных устройств.

Чтобы принадлежность устройств была понятна всем, участникам BYOD следует приобретать личные устройства через обычные розничные сети, а не через отдел закупок организации. Также можно предоставить сотрудникам корпоративные скидки, если с соответствующим поставщиком у компании имеются партнерские связи.

Некоторым сотрудникам может также потребоваться дополнительное оборудование, например мониторы или клавиатура. В этом случае необходимо уточнить, кто будет приобретать и кто будет владеть каждой единицей оборудования.

4. Внедрение

Для успешной реализации крайне важно обеспечить информированность. Предоставьте сотрудникам рекомендации, чтобы помочь им принять решение о целесообразности участия в программе и о том, как выбрать подходящее устройство для своих нужд. Они также должны понимать, как получать, использовать и хранить данные, а также знать соответствующий способ настройки и использования относящихся к работе учетных записей для неуправляемых пользовательских приложений и сервисов.

Рабочие и бизнес-данные должны храниться строго изолированно для соответствия требованиям электронного поиска и политикам защиты данных. Аналогичным образом рабочие электронные письма никогда не должны отправляться из личных почтовых ящиков. Применимые политики использования должны распространяться на личные устройства в той же мере, что и на корпоративные.

Также важно разработать программу адаптации пользователей, которая поможет им быстро приступить к работе. Приветственное электронное письмо со ссылкой на портал самообслуживания поможет сотрудникам быстрее повысить свою продуктивность.

5. Распределение затрат

Сокращение затрат является одним из главных преимуществ концепции BYOD, которая заключается в том, что сотрудники частично или полностью покрывают затраты на различные личные устройства, используемые для работы. Компании, предоставляющие субсидии, обычно предлагают оплату 18–20% стоимости устройства. Участники программы должны быть осведомлены, что любая выплачиваемая субсидия считается доходом, подлежащим налогообложению. В регионах с повышенными ставками индивидуального подоходного налога можно увеличить размер компенсации таким образом, чтобы размер субсидии за вычетом налогов был равным для всех участников программы.

Если будет выплачиваться субсидия, она должна соответствовать всему сроку участия сотрудника. Выплата субсидий должна регулярно продлеваться, чтобы личные устройства не устаревали по сравнению с корпоративными. Если участник увольняется из компании в течение цикла реализации BYOD, вы можете потребовать возвращения части выделенной субсидии.

При внедрении программы BYOD в своей организации помните о последствиях разделения затрат. Одновременное внедрение может повысить расходы, поскольку сотрудники вступают в программу (и востребуют свои субсидии) на любом этапе цикла модернизации конечных устройств. Предлагая сотрудникам вступать в программу в конце срока использования их устройств, вы сможете распределить расходы по времени. С другой стороны, организации, которые не предоставляют субсидий, могут поощрять присоединение к программе с первого дня.

Кроме того, любая политика BYOD с распределением или без распределения затрат должна четко обозначать, кто будет платить за доступ к сети вне сетевой инфраструктуры компании, например по мобильным сетям, через общественные сети Wi-Fi или проводной широкополосный доступ дома.

6. Безопасность и соответствие требованиям регулирующих органов

Важным требованием в отношении как личных, так и корпоративных устройств является защита данных без ущерба для комфортности работы пользователя. Для программ, которые допускают хранение личных приложений и данных на используемых для работы устройствах, управление мобильными приложениями (MAM) позволяет хранить личные и корпоративные приложения и данные отдельно от корпоративного контента.

Установка корпоративных приложений на личные устройства повышает риск. Однако стратегия, сочетающая унифицированное управление конечными устройствами, виртуализацию приложений и десктопов и безопасный обмен файлами, исключает потребность в этом. Коммерческая информация хранится в безопасности в центре обработки данных или в облаке. А в случаях, когда корпоративные данные должны располагаться на мобильном устройстве, их можно защитить путем контейнеризации, шифрования и дистанционного удаления. Вы также можете запретить вывод на печать или доступ к устройствам хранения на стороне клиента, например к локальным дискам и USB-накопителям.

Вы можете обеспечивать контроль и безопасность доступа к приложениям и данным с помощью политик, учитывающих владельца, состояние или местоположение устройства. Вы можете регистрировать любое устройство и управлять им, устанавливать требования к коду доступа, обнаруживать взломанные устройства, а также полностью или выборочно удалять данные с несоответствующих требованиям, утерянных, украденных или принадлежащих уволенным сотрудникам и подрядчикам устройств. Средства обеспечения безопасности приложений включают: безопасный доступ через туннельные соединения, черный список, белый список и динамичные контекстно-зависимые политики.

Для защиты сети можно использовать технологию контроля сетевого доступа (NAC) с целью аутентификации пользователей, подключающихся к сети, и проверки наличия на их устройствах современного антивирусного ПО и патчей безопасности.

За пределами файервола виртуализация и шифрование могут защитить от большинства уязвимостей в системе безопасности Wi-Fi, WEP-шифрования, открытых беспроводных сетей, 3G/4G и других методов доступа потребительского уровня. Средства сетевой безопасности обеспечивают обнаружение и защиту от внутренних и внешних мобильных угроз; блокировку неконтролируемых устройств, неавторизованных пользователей и не отвечающих требованиям приложений; а также интеграцию с системами управления информацией и событиями, относящимися к безопасности (SIEM).

На случай ухода участника программы BYOD из организации, нарушения соответствующей политики, утери или кражи личного устройства у ИТ-отдела должен быть механизм немедленного прекращения доступа к данным и приложениям, включая автоматическую отмену провижининга связанных с работой учетных записей SaaS и выборочное удаление данных на утерянных устройствах. Данная функция также имеет важное значение для устройств COPE и CYOD, позволяя передавать корпоративное устройство новому пользователю и исключая возможность того, что оставшиеся на устройстве данные попадут в руки человека, у которого нет права доступа к ним.

Вместо разрешения реализации открытых подходов BYOD, при которых сотрудники могут использовать любые устройства для доступа к корпоративным приложениям и данным, некоторые организации выбирают управляемый подход. В этом случае ИТ-отдел управляет личными устройствами напрямую, включая регистрацию, проверку, авторизацию и доступ к ресурсам устройства.

7. Мониторинг и управление

Постоянный мониторинг и управление играют ключевую роль в соблюдении политик и определении окупаемости инвестиций.

Некоторые решения UEM повышают продуктивность и эффективность ИТ-инфраструктуры благодаря автоматизации некоторых аспектов мониторинга и управления, например определение действий, которые должны предприниматься в ответ на различные нарушения. Это может быть полное или частичное удаление данных с устройства, настройка устройства как несоответствующего требованиям, изъятие устройства или отправка пользователю уведомления о необходимости устранить нарушение в течение ограниченного периода времени, например, путем удаления приложения, входящего в черный список, прежде чем будут приняты более серьезные меры.

8. Поддержка и обслуживание устройств

Программа BYOD часто сокращает для ИТ-отдела объем обслуживания, необходимый для каждого устройства, потому что пользователь также является и владельцем устройства. Тем не менее политика должна четко определять организацию и оплату различных видов технического обслуживания и поддержки, чтобы избежать увеличения сложности и нагрузки на ИТ-отдел. В рамках большинства программ CYOD и COPE за поддержку и обслуживание устройств полностью отвечает ИТ-отдел.

Как Citrix Workspace обеспечивает безопасное управление устройствами

Любая программа управления устройствами должна включать технологии, обеспечивающие безопасный доступ к корпоративным приложениям и файлам на личных устройствах. Решение Citrix Workspace обладает всеми необходимыми функциями, чтобы сделать концепции BYOD, CYOD и COPE простыми, безопасными и эффективными в любой организации. Оно сочетает в себе функции унифицированного управления конечными устройствами, виртуализации десктопов и приложений Windows, безопасного обмена файлами и доставки приложений для предоставления доступа к корпоративным приложениям и данным на любом устройстве, используемом сотрудниками для работы, при одновременном обеспечении безопасности и контроля.

Унифицированное управление конечными устройствами

Вы можете получить возможности провижининга и управления приложениями, данными и устройствами по уникальным идентификаторам, автоматического отключения учетных записей уволенных сотрудников и избирательного удаления данных на утерянных устройствах. Citrix Workspace не только позволяет вам управлять устройствами, включая Интернет вещей, но также обеспечивает безопасность и

контроль на уровне приложений, поэтому вы можете защищать корпоративные данные, не препятствуя использованию личного контента на устройствах BYOD, CYOD и COPE. Управление конечными устройствами с помощью Citrix Workspace позволяет вам выбирать подходящую для вас стратегию управления мобильными приложениями (MAM): платформенную MAM, например Samsung KNOX или Appconfig, Citrix MDX (которая обеспечивает дополнительный уровень шифрования приложений без регистрации устройств) или Intune MAM.

Виртуализация десктопов и приложений Windows

Вместо того чтобы устанавливать приложения и десктопы Windows и управлять ими на каждом отдельном устройстве, вы можете осуществлять их доставку в виде сервисов по требованию, доступных на любом устройстве. Поскольку управление приложениями и данными осуществляется в центре обработки данных или в облаке, ИТ-отдел может централизованно обеспечивать защиту данных, соответствие стандартам, контроль доступа и администрирование пользователей на личных устройствах так же легко, как и на корпоративных, и в той же самой унифицированной среде.

Магазин приложений

Предоставьте сотрудникам доступ одним нажатием к мобильным, веб-, SaaS-, Windows- и корпоративным приложениям из единого магазина приложений. Независимо от того, какие устройства используют сотрудники — компьютеры Windows или Mac, мобильные продукты на базе iOS, Android или Windows либо устройства Google Chromebook, — комфортность работы пользователей на разных устройствах, в разных местоположениях и сетях остается одинаковой.

Безопасный доступ

Унифицированная структура управления позволяет ИТ-отделу защищать, контролировать и оптимизировать доступ к приложениям, десктопам и сервисам на любом устройстве, а также выполнять аудит и составление отчетов для соблюдения требований регулирующих органов и защиты данных. Только компания Citrix предоставляет уникальную сеть микро-VPN для дополнительной защиты данных приложений между мобильным устройством и корпоративными ресурсами, которые находятся за файерволом.

Безопасный обмен файлами

Сотрудники могут безопасно обмениваться файлами и совместно работать с ними вместе с любым другим лицом в организации или за ее пределами, а также синхронизировать файлы между устройствами. Контроль доступа, аудит, создание отчетов и дистанционное удаление данных на устройствах, выполняемые на основе политик, помогают обеспечить защиту бизнес-данных.

Имея в своем распоряжении надлежащие политики и технологии, вы сможете обеспечить необходимый баланс между свободой выбора для сотрудников и безопасностью и контролем для ИТ-отдела. Узнайте больше, как Citrix Workspace может помочь вам сделать управление устройствами простым и безопасным, на веб-сайте www.citrix.ru/workspace

Отдел продаж
Северная Америка | 800-424-8749
Другие страны | +1 408-790-8000

Офисы
Штаб-квартира | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States