vmware®

Рекомендации экспертов

10 советов по обеспечению безопасности развертывания VMware Horizon

Обеспечение безопасности ИТ-среды в эпоху виртуализации

Привлеченные высоким уровнем мобильности виртуальных сред следующего поколения ИТ-отделы стремятся избавиться от ограничений традиционной архитектуры. VMware® Horizon® преобразует среду настольных компьютеров, в результате конечные пользователи получают гибкие возможности доступа к виртуализированным компьютерам и приложениям на основе единой платформы.

Однако с новыми возможностями, такими как использование личных устройств на работе, появляются и новые трудности с обеспечением ИТ-безопасности. Для расширенного доступа требуется повышенная бдительность, чтобы данные оставались в безопасности. Число инцидентов увеличивается на 66% в год, а средние расходы в результате нарушения безопасности составляют 5,9 млн долларов[1], поэтому преобразование среды настольных компьютеров должно быть одновременно эффективным и безопасным.

ЧТО ПРЕДСТАВЛЯЕТ СОБОЙ VMWARE HORIZON?

Решение VMware Horizon расширяет возможности виртуализации, предоставляя конечным пользователям виртуализированные настольные компьютеры и приложения на основе единой платформы. Доступ к этим виртуальным компьютерам и приложениям (включая размещенные приложения на базе RDS и приложения, упакованные с помощью VMware ThinApp®) осуществляется из единой рабочей области на любых устройствах, в любой точке и для всех типов подключения. Чтобы получить дополнительные сведения о Horizon, посетите веб-сайт vmware.com/go/horizon.

Появление новых задач в области ИТ-безопасности в результате виртуализации пользователей

Преобразование среды настольных компьютеров предоставляет множество преимуществ конечным пользователям и ИТ-отделам, таких как сокращение эксплуатационных и капитальных расходов, упрощенное управление, повышение производительности пользователей и высокая доступность, однако при этом необходимо учитывать новые возможные проблемы.

- Благодаря возможностям предоставления приложений и виртуальных компьютеров в режиме реального времени, полученным за счет преобразования среды настольных компьютеров, ИТ-администраторы смогут за считаные секунды предоставлять новым пользователям виртуальные компьютеры без сохранения состояния. Возможность быстрого развертывания при сохранении визуализации или контроля над сетью

- Ваша организация может обслуживать тысячи и даже сотни тысяч пользователей, которые работают с важной инфраструктурой. Если безопасность виртуальных компьютеров будет нарушена, этот инцидент может дорого обойтись организации.

- Горизонтальный трафик, который передается между внутренними серверами или настольными компьютерами, может сделать среду уязвимой. Повседневные действия проверенных конечных пользователей могут представлять собой угрозу сети, например просмотр зараженных вирусом электронных сообщений или переход по вредоносной ссылке на веб-сайте.

Исходя из этого, мы составили список из 10 рекомендаций, которые помогут вам обеспечить безопасность среды Horizon.

1 Использование эталонных образов

С помощью единого шаблона в виде эталонного образа ИТ-отделы могут адаптировать виртуальные настольные компьютеры, чтобы пользователи видели только операции, связанные с бизнес-потребностями. При этом ИТ-специалисты смогут уделять основное внимание поддержанию чистоты эталонного образа, который будет храниться в ЦОД в полной безопасности. Если виртуальный компьютер скомпрометирован, ИТ-отдел может удалить образ и выполнить развертывание на новом компьютере.

2 Использование многоуровневой системы безопасности

В виртуализированной среде необходимо бороться с угрозами безопасности на нескольких фронтах. Принимая дополнительные меры, например создавая список допустимых приложений в VMware NSX™, можно напрямую выбирать приложения, которые будут работать в сети. Этот механизм обеспечивает безопасность сети и соответствие пользователей нормативным требованиям, что играет важную роль на фоне распространения «теневых» ИТ-услуг, когда конечные пользователи и руководители подразделений используют бизнес-приложения и услуги за пределами ИТ-домена. Целостность приложений также можно обеспечить с помощью надежных методов предоставления приложений, используя такие средства, как VMware App Volumes™.

1. PwC, Managing cyber risks in an interconnected world («Управление виртуальными рисками во взаимосвязанном мире»), сентябрь 2014 г.

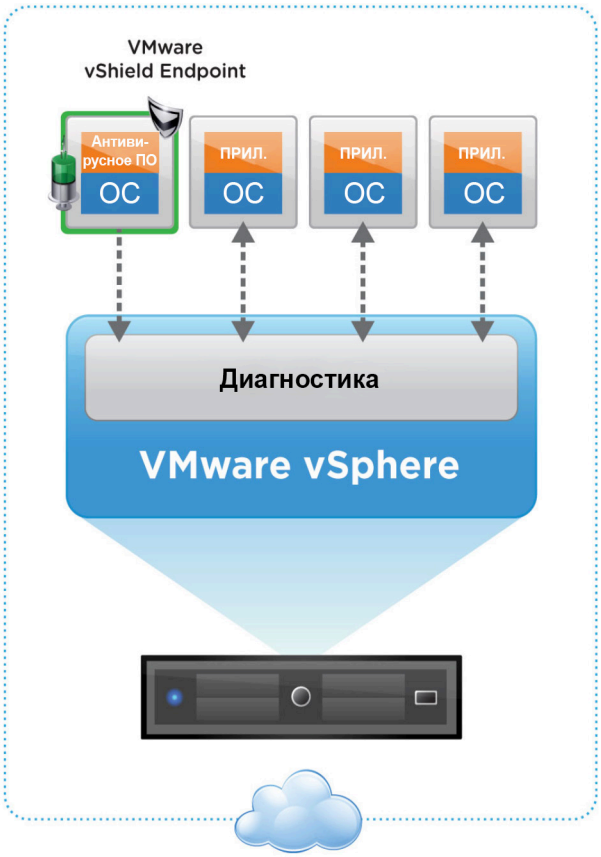
СВЕДЕНИЯ О РЕШЕНИИ VMWARE APP VOLUMES

С помощью VMware App Volumes ИТ-администраторы могут предоставлять приложения и данные пользователям или на виртуальные компьютеры за считаные секунды и с возможностью масштабирования. App Volumes помогает сократить расходы на инфраструктуру и управление благодаря использованию управляемых томов. С точки зрения конечных пользователей приложения ведут себя как стандартные, что обеспечивает оптимальные условия работы на разных устройствах и в различных сеансах.

Преимущества:

- Централизованное управление приложениями
- Удобное развертывание приложений
- Предоставление приложений на уровне пользователей

Дополнительные сведения о решении App Volumes см. на странице https://www.vmware.com/ru/products/appvolumes/.



3 Использование надежных методов обеспечения безопасности конечных устройств

Вкладывая средства в оборудование и программное обеспечение, можно повысить уровень безопасности конечных устройств Horizon. Например, если устройство будет потеряно или украдено, аппаратные возможности, такие как Trusted Platform Module (TPM), не допустят загрузки устройства благодаря встроенной проверке подлинности. Необходимо непрерывно обновлять определения антивирусной системы и антивредоносное ПО, а также следить за обновлением и работой брандмауэра устройств.

Некоторые ИТ-администраторы не следуют рекомендациям по антивирусной защите на виртуальных компьютерах, чтобы снизить уровень использования памяти, ресурсов ЦП и дисков. Однако негативные последствия, вызванные вирусом на виртуальном компьютере, могут быть такими же серьезными, как и на физическом компьютере, особенно если виртуальные машины не обновляются на регулярной основе. Решение VMware vShield Endpoint™, которое переносит средства защиты от вирусов и вредоносного ПО с виртуальных машин на безопасное виртуальное устройство, может стать превосходной альтернативой.

Наконец, можно повысить уровень безопасности конечных устройств с помощью сторонних решений. Различные поставщики, например Trend Micro Deep Security, предоставляют дополнительные возможности для защиты от вредоносного ПО, обнаружения и предотвращения вторжений, мониторинга целостности, фильтрации URL-адресов и установки исправлений. Расширенные возможности обеспечения безопасности используются на уровне гипервизора и обеспечивают мгновенную защиту с момента инициализации нового виртуального компьютера. Кроме того, средства безопасности автоматически переносятся вместе с конечным устройством при его перемещении в ЦОД.

СВЕДЕНИЯ О РЕШЕНИИ VMWARE VSHIELD ENDPOINT

VMware vShield Endpoint укрепляет защиту виртуальных машин и многократно увеличивает производительность средств защиты конечных устройств. Решение vShield Endpoint использует существующую инфраструктуру и помогает заказчикам управлять антивирусными и антивредоносными политиками для виртуализированных сред в том же интерфейсе, который используется для защиты физических сред. Это решение интегрируется с продуктами следующих поставщиков: Trend Micro, Intel Security, Symantec, Sophos и Kaspersky.

4 Реализация групповых и расширенных политик

При нарушении безопасности конечного устройства, например при отсутствии обновлений антивирусного или антивредоносного ПО, групповые политики помогут избежать неприятностей. С помощью групповой политики можно обеспечить согласованность среды виртуальных компьютеров, отключить лишние службы и отключить доступ к определенным компонентам виртуального компьютера или сети. Параметры политики также не разрешают пользователям вносить изменения, которые могут сделать виртуальные компьютеры уязвимыми.

Кроме того, рассмотрите возможность использования VMware User Environment Manager™, удобного, мощного и масштабируемого решения по управлению средами пользователей, которое помогает ИТ-специалистам администрировать приложения и пользователей, а также настраивать динамические политики. Повседневные ИТ-процессы становятся эффективнее и безопаснее, если политики и параметры приложений следуют за пользователями в различных точках и на разных устройствах, при этом пользователям предоставляются определенные права доступа в зависимости от того, работают ли они на внутреннем настольном компьютере или внешнем устройстве.

Кроме того, используя файлы шаблонов администрирования групповых политик (ADM) Horizon, которые дополняют групповую политику Active Directory, можно регулировать передачу и получение данных на виртуальном компьютере, например отключить буфер обмена.

5 Обеспечение надлежащей архитектуры

При использовании Horizon необходимо внимательно следить за конфигурацией брандмауэра и ДМЗ, а также за разделением пулов виртуальных компьютеров. На первом этапе следует разместить брандмауэр между сетью ЦОД и офисной сетью. Если виртуальные локальные сети или брандмауэры используются для распределения серверов и настольных компьютеров по разным сегментам, среда инфраструктуры виртуальных компьютеров должна быть размещена там же, где и настольные компьютеры.

Для обеспечения безопасности удаленных пользователей следует настроить сервер безопасности или точку доступа в ДМЗ. Таким образом пользователи получат точку соединения, но без прямого доступа к сети. В качестве шлюза можно использовать решение Access Point на сервере безопасности, которое предоставляет множество преимуществ. Вместе с Access Point заказчики получают заблокированную виртуальную машину на базе Linux с надежной системой безопасности и предварительно настроенной конфигурацией, а не просто программное обеспечение, которое выполняется в стандартной ОС Windows. Кроме того, Access Point можно присоединить к отдельному серверу подключений View или средству балансировки нагрузки, размещенному перед несколькими серверами подключений View для обеспечения высокой доступности.

Разделение пулов виртуальных компьютеров рекомендуется, если часть из них, например виртуальные компьютеры для отдела кадров, подрядчиков или разработчиков, должны быть отделены от организации. Используя VMware NSX в качестве дополнительного модуля для платформы VMware vSphere®, можно добиться такого разделения.

6 Использование многоуровневой и сквозной проверки подлинности

Продукт Horizon совместим с ведущими решениями многоуровневой проверки подлинности, такими как RSA SecurID, VASCO DIGIPASS, SMS Passcode и SafeNet, поэтому он служит эффективной основой для обеспечения надежной защиты виртуальных компьютеров. Кроме того, Horizon поддерживает процедуру сквозной проверки подлинности, в рамках которой пользователи вводят учетные данные дважды или входят в систему виртуального компьютера с отдельной учетной записью.

Кроме того, рассмотрите возможность использования VMware Identity Manager™. Это решение по управлению учетными данными обеспечивает условный доступ и единый вход, что помогает упростить поддержку мобильных технологий и улучшить условия работы пользователей на различных устройствах без ущерба для безопасности среды.

7 Защита периферийных устройств

Внешние диски могут использоваться для распространения вирусов и даже для кражи интеллектуальной собственности. Решение Horizon предотвращает копирование данных на локальные портативные устройства, например USB-накопители и незащищенные принтеры. Кроме того, если компонент перенаправления клиентских дисков установлен на виртуальном компьютере, с его помощью пользователи могут получить удаленный доступ к файлам, которые хранятся на локальном ПК. Сжатие и шифрование осуществляются при передаче файлов с конечного устройства на виртуальный компьютер.

8 Периодическое обслуживание и проверка

Забота о безопасности характеризуется внимательным отношением к обслуживанию. Выполнение следующих действий поможет предотвратить ущерб от потенциальных угроз.

- Обновление антивирусных и антивредоносных компонентов ПО, которые уведомляют сотрудников об атаках.
- Определение эффективной политики регулярного изменения или обновления конфигурации виртуальных компьютеров Horizon для установки исправлений системы безопасности и приложений, а также обновлений операционной системы.
- Регулярные исправления и обновления системы безопасности не только для ОС, но и для приложений в эталонном образе.
- Периодические проверки основного и дополнительного брандмауэра для обеспечения корректного применения политики брандмауэра и предотвращения несанкционированного доступа к ДМЗ.
- Анализ потока трафика, чтобы понять, какой трафик попадает в брандмауэры и ДМЗ, а также отслеживание неиспользуемых портов брандмауэра.
- Регулярные аудиты. В частности, следует периодически проводить аудит конфигурации средства балансировки нагрузки и брандмауэра, чтобы убедиться в отсутствии несанкционированного доступа.
- При установке обновлений и исправлений сначала следует обновить родительский образ, протестировать его, а затем быстро развернуть этот образ на все виртуальные компьютеры.

ЗАЧЕМ НЕОБХОДИМО ОБНОВЛЕНИЕ? ПОВЫШЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ

Обновление виртуальных компьютеров при выходе из системы обеспечивает каждому пользователю чистый и работоспособный виртуальный компьютер. В дополнение к повышенному уровню безопасности (из-за удаления возможных вирусов и вредоносного ПО с виртуального компьютера) следующий пользователь получает все необходимые возможности с улучшенной производительностью.

9 Обеспечение безопасности сети

Совместное использование решений VMware NSX и Horizon обеспечивает возможность автоматизации и микросегментации. С помощью VMware NSX можно развернуть распределенный брандмауэр для отдельных портов, чтобы контролировать трафик, получаемый виртуальным компьютером, а также отправителей и получателей трафика. Кроме того, можно создать зоны для изоляции подрядчиков и защиты сети от потенциальных веб-угроз.

При использовании микросегментации каждой виртуальной машине выделяется собственный защитный периметр. Распределенный брандмауэр отслеживает трафик, передаваемый и получаемый каждой ВМ, предотвращая несанкционированный доступ и защищая ЦОД от угроз. Путем автоматизации рабочих нагрузок инициализации системы безопасности и микросегментации можно добиться более быстрого и надежного масштабирования, а также повысить производительность виртуальных компьютеров.

10 Предоставление только необходимого доступа

Никогда не оставляйте уязвимые места, которыми могут воспользоваться другие. Для этого необходима детализация разрешений доступа. В стандартной среде приложения могут получать доступ к другим приложениям. При наличии вредоносного ПО одно приложение может записать данные в область памяти другого приложения. Это может привести к серьезным последствиям, так как все данные, к которым это приложение обращается, могут быть скомпрометированы. VMware ThinApp обеспечивает виртуализацию приложений, каждое из которых получает собственную изолированную среду виртуальной ОС. При этом приложения не могут получать доступ к файлам других приложений, а определенные части ОС можно полностью изолировать от приложений. В результате ограничивается область действия потенциальной угрозы, которую быстро можно будет устранить в случае нарушения.

СТАНДАРТНЫЕ РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ, КОТОРЫЕ ИНОГДА ИГНОРИРУЮТ.

- По возможности не предоставляйте пользователям права администратора.
- Относитесь к виртуальным компьютерам как к традиционным с точки зрения безопасности, применяя политики и используя антивирусное ПО и средства изоляции.
- Замените стандартные самозаверенные сертификаты для защиты SSL-каналов на один сертификат, созданный надежным центром сертификации, чтобы снизить вероятность атак через посредника.
- Если для удаленного доступа пользователям необходим второй виртуальный компьютер, следует ограничить их доступ к конфиденциальным данным.
- Используйте решение VMware vRealize® Operations Manager™ для мониторинга пиков трафика.
- Для внешнего развертывания следует разместить серверы безопасности или серверы Access Point в ДМЗ.

Заключение

Несмотря на обещанную гибкость конечных пользователей и эффективное управление, преобразование настольных компьютеров не повысит уровень безопасности ИТ-отдела автоматически. Как отмечалось выше, организация может столкнуться с дополнительными проблемами, если заранее не примет соответствующих мер. Корректная реализация и соблюдение рекомендаций, представленных в этом документе, помогут обеспечить безопасность сети и предоставить все преимущества преобразования настольных компьютеров.

Вы можете испытать Horizon бесплатно на практическом занятии. Тестовая среда будет готова к работе через браузер за считаные минуты без установки какого-либо ПО. Регистрация: https://www.vmware.com/horizon-hol-labs.

Следите за нашими новостями

Блог: https://blogs.vmware.com/euc

Twitter: @vmwarehorizon

Facebook: https://www.facebook.com/vmwarehorizon

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel (877) 486–9273 Fax (650) 427–5001 www.vmware.com
125284, Россия, Москва, ул. Беговая, д. 3/1. Тел.: +7 (495) 212–2900 Факс: +7 (495) 212–2901 www.vmware.ru