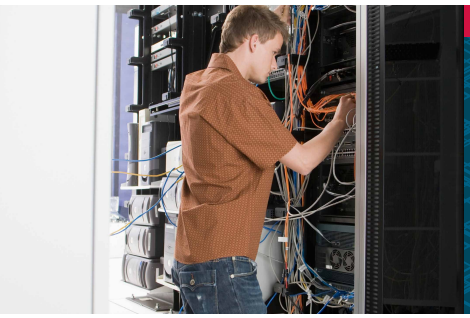

Расширение виртуальной среды и обеспечение безопасности

Ключевые решения по обеспечению безопасности виртуальных инфраструктур

По мере того как роль виртуализации становится критически важной для серверов и рабочих станций, ИТ-отделам приходится поддерживать все больше конечных пользователей, все большую рабочую нагрузку, все больший территориальный охват, а также обеспечивать новые требования, такие как подготовку сервисов к работе «ко времени» (just in time provisioning) и создание системы самообслуживания. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) позволяет создавать системы безопасности, учитывающие индивидуальные технические характеристики виртуальных сред и особенности управления ими. Это решение позволяет достичь желаемого уровня эффективности без ущерба для безопасности, существенно увеличивая уровень удовлетворенности пользователей при работе в виртуальной среде.

Внедрение технологий виртуализации стало главным приоритетом для руководителей ИТ-подразделений в 2012 г.[1] Благодаря поддержке ключевых программ, таких как «облачные» вычисления, использование личных устройств сотрудников на рабочем месте и консолидация серверов и центров обработки данных, виртуализация позволяет предприятиям одновременно повысить организационную гибкость и сократить расходы. Виртуализация стала критическим фактором успеха. Но в то же время виртуализация сопряжена с значительными проблемами управления рисками и обеспечения операционной безопасности по сравнению с традиционными системами обеспечения безопасности физических устройств. Новая операционная модель виртуализации требует переоценки традиционных производственных процессов, политик и вариантов развертывания систем безопасности.

«Узкие места» производительности

Наиболее очевидной проблемой является производительность процессов сканирования. При традиционном развертывании каждая система (рабочая станция или сервер) эксплуатирует средства защиты от вредоносных программ локально, выполняя сканирование при доступе или по графику, обеспечивая безопасность узла. Однако при использовании в виртуальных средах такая модель является чрезвычайно ресурсоемкой. При возникновении так называемых «шквальных» сканирований (scan storms) операции сканирования могут забрать все ресурсы памяти и процессора гипервизора, блокируя новые пользовательские сеансы. Чтобы сохранить требуемый уровень производительности, многие администраторы просто отключали процессы сканирования или отменяли установку обновлений ПО.

Однако, по мере того, как виртуальные среды становились основной платформой коммерческих предприятий, они превращались в мишень для атак киберпреступников, использующих уязвимости программного обеспечения и конфигурации. Без своевременного и активного сканирования виртуальная инфраструктура представляет собой лакомый кусок для злоумышленников и охотников за данными.

Необновленные защитные программы

Первой целью киберпреступников являются образы, работающие без обновленных программ, а нередко вообще без программ защиты от вредоносных программ. Защитное ПО должно присутствовать как на работающих образах, так и на образах, находящихся в автономном режиме, включая шаблоны образов (или «золотые образы»). Только своевременно обновленные функции системной безопасности и средства защиты от вредоносных программ могут обеспечить эффективное отражение атак злоумышленников.

В результате масштабирования инфраструктуры виртуальных машин (VDI) количество виртуальных машин вашей сети может достигать тысяч, каждая из которых включается и выключается каждый день, что делает задачу по обслуживанию системы безопасности менее предсказуемой. Если постоянно работающие физические серверы могут быть настроены на выполнение обновлений систем безопасности в удобное время, т. е. когда степень их использования низка, то пользователи рабочих станций должны выполнять такие обновления с учетом динамики рабочих процессов виртуальных машин. Текущие образы переводятся в автономный режим и сохраняются на ночь или на несколько часов, будучи неактивными, затем пользователи ожидают получения немедленного доступа к своим виртуальным системам без задержки на загрузку и сканирование.

Смешение активов

Центры обработки данных усложняют процесс. Серверные и сетевые ресурсы, а также ресурсы хранения объединяются в целях максимального увеличения эффективности, однако такое совмещение имеет два побочных эффекта. Во-первых, вы теряете преимущество обеспечения безопасности за счет физического разделения банков данных, серверов приложений, веб-серверов и другого ПО. Физическая изолированность существенно ограничивает возможности распространения вредоносных программ, к неудовольствию их авторов и хакеров. Чтобы компенсировать этот недостаток, для виртуальных систем должна быть разработана более мощная система защиты.

Во-вторых, следует изменить сам процесс управления, поскольку ранее раздельные функции серверов, хранения и сетевые функции теперь объединены в одной консоли управления. Если раньше такие ресурсы имели различных администраторов и различные политики, то теперь следует обеспечить их сосуществование в рамках единой среды, регулирующей политики и процедуры, которая обычно управляется одним администратором виртуальной среды, так называемым «суперпользователем». В такой ситуации появляется проблема конкуренции процессов и предупреждений, которая усложняет представление информации для задач управления. Кроме того, порой возникает необходимость стандартизировать политики. Администраторам следует разработать пути оперативного взаимодействия.

«Антивирус McAfee MOVE [AntiVirus] AV обеспечивает McKesson всеобъемлющую и стабильную защиту наших виртуальных сред от вредоносного кода. Поскольку мы продолжаем внедрять новые технологии, в частности «облачные» решения, использование антивируса McAfee MOVE [AntiVirus] AV обеспечивает дополнительную безопасность в нашей виртуальной среде. Это решение значительно облегчает масштабирование и развертывание и гарантирует, что все развернутые системы имеют одинаковый уровень защиты»,

— Патрик Эньярт (Patrick Enyart)
Старший директор
McKesson Information Security

Различные поставщики

Помимо вышеперечисленных аспектов немало организаций сталкиваются с проблемой наличия нескольких поставщиков. Различные поставщики решений для виртуализации имеют свои плюсы и минусы, поэтому многим компаниям требуется дополнительный поставщик критически важного ПО. В результате развернутая система представляет собой комбинацию гипервизоров. Вы должны обеспечить защиту образов и создавать отчеты о нормативно-правовом соответствии с учетом различных атрибутов каждого гипервизора.

Нормативно-правовое соответствие

И завершая этот, казалось бы, уже достаточно длинный список проблем, вам необходимо подтвердить, что ваши виртуальные системы соответствуют нормативно-правовым требованиям, которые применялись — и все еще продолжают применяться — к физическим системам. Современные нормы требуют регулярного обслуживания программ защиты от вредоносных программ. Так, закон штата Массачусетс о конфиденциальности данных (Massachusetts Data Privacy Law 201 CMR 17:00) требует использовать «достаточно актуальные версии программного агента обеспечения безопасности систем, которые должны включать защиту от вредоносных программ, достаточно актуальные обновления и антивирусные базы, или версии такого программного обеспечения, которые поддерживаются актуальными обновлениями и антивирусными базами, и которые настроены на регулярное получение актуальных обновлений защиты».

Перечисленные проблемы представляют сложности практического характера при выполнении повседневных операций обеспечения безопасности в условиях быстро меняющихся угроз. Традиционные модели обеспечения безопасности, использовавшиеся в мире физических устройств, должны быть дополнены или же заменены решениями, оптимизированными для виртуальных сред.

Оптимизация работы благодаря решению McAfee MOVE

Когда несколько лет назад компания McAfee начала сотрудничество с разработчиками решений виртуализации, мы стали свидетелями возникновения проблем обеспечения безопасности. Нашим ответом на эти проблемы стала специализированная технология, позволяющая реализовать лучшие функции защиты McAfee в условиях виртуальных серверов и рабочих станций. McAfee MOVE AntiVirus предлагает защиту от вредоносных программ и безопасность без ущерба для производительности. Вы получаете максимальные возможности мощной технологии виртуализации и одновременно сохраняете производительность пользователей и безопасность гостевой операционной системы на виртуальной машине.

Наше решение обеспечивает гибкость, предлагая выбор предпочитаемой модели развертывания, например, такой, которая может работать на базе различных платформ виртуализации, или в безагентной версии, использующей прикладные программные интерфейсы VMware vShield. Оба варианта полностью используют все преимущества зарекомендовавшей себя передовой[2] защиты McAfee от вредоносных программ. Кроме того, средства защиты веб-приложений и предотвращения вторжений обеспечивают дополнительный уровень защиты от вредоносных атак.

Сканирование по возможности и только при необходимости

McAfee MOVE AntiVirus высвобождает ресурсы гипервизоров для реализации других задач, гарантируя при этом регулярное выполнение сканирования безопасности в соответствии с политикой организации. Отказоустойчивое виртуальное или физическое устройство берет на себя обработку запросов на сканирование, обслуживание конфигураций и обновление DAT-сигнатур, позволяя гипервизору сосредоточить все свои ресурсы на обслуживании гостевых образов.

Интеграция McAfee MOVE AntiVirus с программой управления виртуализацией позволяет избежать «шквальных» сканирований, которые провоцируются при одновременных запросах нескольких образов на предоставление доступа и сканирование. Кроме того, решение McAfee MOVE AntiVirus for Virtual Servers способно осуществлять интеллектуальное планирование сканирований в зависимости от загруженности гипервизора и доступности ресурсов. Для выполнения сканирования не требуется перевода виртуальных машин в автономный режим. Однако, после отключения образов от системы, решение McAfee может выполнить их сканирование и обновление, всегда сохраняя их в состоянии полной готовности к использованию.

Использование новейших разработок

McAfee MOVE AntiVirus осуществляет защиту виртуальных машин с помощью того же ядра McAfee VirusScan®, что и наши передовые продукты антивирусной защиты для физических устройств. Чтобы сканирование осуществлялось как можно более своевременно, но не снижало производительность, приложение выполняет загрузку и ввод последних обновлений сигнатур на выделенный скан-сервер, а не на индивидуальные виртуальные машины. McAfee MOVE AntiVirus обращается к ресурсам технологии McAfee Global Threat Intelligence™ для проверки в режиме реального времени репутации неизвестных файлов, которые вызывают подозрения.

Кроме функции сканирования на наличие вредоносных программ решение McAfee MOVE AntiVirus for Virtual Desktops включает межсетевой экран для рабочих станций и передовую технологию защиты памяти, которые предотвращают вредоносные действия и сохраняют целостность файлов. Чтобы помочь пользователям избежать посещения сомнительных веб-сайтов, способных в ходе работы стать источниками заражения образа вредоносными программами, в решение McAfee также включены предупреждения о репутации веб-сайта и инструменты контроля за посещением веб-страниц с помощью политик. Вместе все эти инструменты позволяют снизить контактную зону для атак на ваши виртуальные системы. Для обеспечения наиболее мощной защиты решение может включать и такие инструменты, как белые списки приложений, которые не позволяют нежелательным приложениям и вредоносным программам нарушить работу систем.

Безопасность в сети

Виртуализация, помимо всего прочего, изменяет подход организаций к обеспечению сетевой безопасности. При виртуализации физической инфраструктуры для создания и соблюдения границ безопасности при отсутствии физического разделения необходимы новые стратегии. Другой проблемой является мобильность виртуальных машин и ее влияние на политики сетевой безопасности. Организациям необходимо решение для постоянного обеспечения сетевой безопасности независимо от места физического расположения виртуального приложения или сервера.

McAfee предлагает интегрированную сетевую систему безопасности для физических и виртуальных сред. Благодаря полной интеграции с интерфейсом сетевой безопасности API системы VMware vShield платформа McAfee Network Security Platform имеет встроенную функцию инспекции виртуальных сред. Она позволяет вам выполнять проверку трафика и обеспечивать принудительное применение политик на виртуальных машинах и между ними, независимо от их физического местонахождения. Кроме того, встроенная функция доступа к инструментам VMware vCenter позволяет интегрировать средства защиты сети в виртуальных средах.

Комплексное управление

McAfee MOVE AntiVirus использует ту же среду управления McAfee ePolicy Orchestrator® (McAfee ePO™), уже знакомую администраторам по инструментам McAfee для обеспечения защиты физических конечных точек, данных и сети. С помощью единой системы политик и консоли управления любой администратор может создавать индивидуальные панели управления для отслеживания интересующих его данных и действий и создавать отчеты по специальным активам, включая совмещение физических и виртуальных узлов — как конечных точек, так и серверов. Такая поддержка различных ролей облегчает адаптацию системы безопасности к объединенной административной среде виртуальных центров обработки данных. Программное обеспечение McAfee ePO также интегрируется с более чем 100 продуктами партнеров McAfee по программе технологического сотрудничества McAfee Security Innovation Alliance, позволяя ИТ-отделам оптимизировать рабочие процессы всей инфраструктуры ИТ.

Стандартизация или специализация

Возможность выбора между многоплатформенным развертыванием и развертыванием, не требующим установки агента, означает, что вы можете поддерживать совместимость с продуктами как уже имеющихся, так и новых поставщиков. В многоплатформенном решении используется «легковесный» агент, запускаемый в каждом гостевом образе для управления политиками и сканированием и реализующий преимущества выделенного скан-сервера для сканирования при обращении. Такой подход позволяет совмещать гипервизоры Citrix, VMware, и Microsoft, обеспечивая бóльшую гибкость и возможность удовлетворить требования различных групп пользователей.

Наша безагентная альтернатива очень тесно интегрирована с платформой VMware и позволяет добиться максимальной отдачи от инвестиций в технологии гипервизора. McAfee MOVE AntiVirus работает через компонент VMware vShield Endpoint, сканируя виртуальные машины «снаружи» гостевого образа при полном отсутствии какого-либо программного обеспечения McAfee на самом образе. Просканированные виртуальные машины могут с помощью технологии VMware vMotion мигрировать с одного узла на другой, не влияя на работу пользователей или сканирующие системы. Интеграция McAfee ePO с инструментом vCenter позволяет максимально оптимизировать процессы контроля и управления инцидентами безопасности.

Непрерывное нормативно-правовое соответствие

Единая платформа McAfee ePO позволяет вам гарантировать согласованность политик как в виртуальных, так и в физических системах. В целях поддержки процессов обеспечения нормативно-правового соответствия вы можете создать представление для аудитора для просмотра релевантных данных и составления запланированных и не запланированных отчетов в зависимости от конкретных нормативных требований.

Шаг вперед

Теперь вы можете обеспечить соответствие системы безопасности требованиям виртуализации. Компания McAfee оптимизировала свои средства защиты от вредоносных программ и конечных точек с учетом специфики внутренних и внешних особенностей архитектуры и процессов, стремясь обеспечить максимально эффективную виртуализацию. Сканирование не препятствует работе активных пользователей, при этом программы системы безопасности и процессы обновления сигнатур учитывают специфику образов рабочих станций и серверов, находящихся то в сети, то не в сети.

Наш гибкая архитектура позволяет вам работать с предпочитаемыми вами поставщиками, тем не менее обеспечивая соблюдение стандартов безопасности и нормативно-правового соответствия. McAfee помогает вам воспользоваться всеми преимуществами виртуализации, надежно защищая ваших пользователей и ваши данные от современных киберпреступников. Мы продолжаем инвестировать в интеграцию и оптимизацию широкого спектра наших продуктов для того, чтобы при расширении виртуальных сред в вашем распоряжении находилась самая мощная и самая эффективная система защиты.

Для получения подробной информации о решении McAfee MOVE AntiVirus посетите веб-сайт www.mcafee.com/ru/solutions/virtualization/virtualization.aspx или же обратитесь к своему региональному представителю или реселлеру McAfee.

McAfee
An Intel Company

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

[1] http://www.informationweek.com/news/storage/virtualization/232400150
[2] http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2011.pdf

45601brf_virtualization_0512_fnl_ETMG