McAfee Security Suite for Virtual Desktop Infrastructure

Защита, которая вам нужна, и гибкость, которую вы заслуживаете

В настоящее время наблюдается переход на использование виртуальных рабочих столов (VDI). Однако в используемые для этого решения должны быть изначально встроены надежные средства защиты. Только так компании смогут защитить себя от угроз без снижения уровня быстродействия и без отказа от требуемой плотности серверов. Традиционные антивирусные программы не очень хорошо интегрируются в виртуальную инфраструктуру. Как справиться с этой проблемой? С помощью комплекта McAfee® Security Suite for VDI, обеспечивающего комплексную защиту, оптимизированную для виртуальных рабочих столов.

Ключевые преимущества

- Обнаружение виртуальных столов и сбор информации о них в средах VMware vSphere с помощью программного обеспечения McAfee ePO и McAfee Data Center Connector for VMware vSphere. Уникальное сочетание белых и черных списков обеспечивает защиту физических и виртуальных серверов от вредоносных программ.
- Оптимизированная защита виртуальных сред, отличающаяся минимальным снижением уровня быстродействия.
- Защита от неизвестных угроз благодаря запрету запуска нежелательных приложений на виртуальных рабочих столах.
- Дополнительные средства защиты от вторжений и веб-атак: брандмауэр для рабочих столов, средства защиты памяти и веб-приложений.
- Использование программного обеспечения McAfee ePO дает возможность быстро собирать информацию, управлять средствами защиты и генерировать отчеты по всем конечным точкам.

McAfee Security Suite for VDI обеспечивает антивирусную защиту, оптимизированную для виртуальных рабочих столов, дает возможность использовать белые списки для защиты от угроз «нулевого дня» и обеспечивает защиту от вторжений на рабочие столы и защиту данных. Решение также предупреждает пользователей о вредоносных веб-сайтах и/или блокирует доступ к ним.

Оптимизированная архитектура сканирования

Динамический характер виртуальных рабочих столов требует осторожного подхода. В автономном режиме в образах не должно быть вредоносных программ, а в момент начала пользовательского сеанса следует обеспечить их немедленное сканирование. Следует учесть, что служба защиты от вредоносных программ — не единственная запускаемая служба, а если пользователи начинают работу одновременно, то происходят резкие скачки нагрузки — так называемые «антивирусные штормы», которые расходуют все ресурсы и лишают пользователей доступа к сеансу.

Чтобы устранить вызываемые сканированием «узкие места» и задержки, McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus перераспределяет операции сканирования файлов, настройки защиты и обновления DAT-файлов с отдельных гостевых образов на отказоустойчивое виртуальное устройство/сервер сканирования с оптимизацией нагрузки (Offload Scan Server). Мы создаем и обслуживаем глобальный кэш сканированных файлов, благодаря чему после сканирования файла и подтверждения отсутствия в нем вредоносного кода другим виртуальным машинам при доступе к этому файлу уже не придется ожидать результатов сканирования. Это позволяет снизить ресурсы памяти, выделяемые для каждой виртуальной машины, что увеличивает общий объем свободных ресурсов и способствует повышению эффективности их использования. Сканирование по требованию осуществляется в режиме автоматизированного планирования и поэтому не влияет на быстродействие гипервизора.

intel Security

Конфигурация McAfee Security Suite for VDI

McAfee MOVE AntiVirus for Virtual Desktops (VDI)

- McAfee MOVE AntiVirus
  - Мультигипервизорное развертывание
  - Безагентное развертывание
- McAfee Data Center Connector for VMware vSphere
- McAfee VirusScan® Enterprise for Windows (ПО)
- McAfee VirusScan Enterprise for Linux (ПО)
- McAfee Host Intrusion Prevention System
- McAfee Application Control for Desktops
- McAfee SiteAdvisor® Enterprise (технология)
- McAfee ePolicy Orchestrator (ПО)

Управление с помощью настраиваемых политик

Программная консоль McAfee® ePolicy Orchestrator® (McAfee ePO™) дает возможность настраивать политики и элементы управления, позволяющие управлять поведением McAfee MOVE AntiVirus. Данные с виртуальных рабочих станций могут быть объединены с данными других систем в рамках единых панелей мониторинга и отчетов. С помощью McAfee Data Center Connector администраторы могут создавать индивидуальные политики для виртуальной машины, совокупности ресурсов, кластера или центра обработки данных в соответствии с требованиями обеспечения защиты конкретного центра обработки данных.

Использование VMware vShield в варианте безагентного развертывания для повышения эффективности

В случае безагентного развертывания компонент VMware vShield Endpoint использует гипервизор в качестве высокоскоростного соединения, позволяя виртуальному устройству McAfee MOVE AntiVirus Security Virtual Appliance (SVA) выполнять сканирование виртуальных машин, находясь за пределами гостевого образа. По мере сканирования vShield по указанию устройство SVA отправляет в кэш доброкачественные файлы и удаляет или блокирует вредоносные файлы, либо помещает их в карантин.

Установив и настроив устройство SVA и необходимые компоненты vShield на серверах ESX, а также установив драйвер vShield на гостевых виртуальных машинах, вы обеспечите автоматическую защиту каждого образа с момента его создания. Это позволяет не устанавливать программное обеспечение McAfee на каждую клиентскую виртуальную машину. В нашем решении реализуются возможности технологии vMotion, т. е. вы можете переносить свои виртуальные машины с одного узла на другой, и при этом устройство SVA гарантирует их непрерывную защиту на целевом узле без замедления сканирования и без нарушений в работе пользователей. Высокая степень интегрируемости решений McAfee позволяет просматривать состояние виртуального устройства SVA в vCenter и получать предупреждения в случае потери связи с SVA, а при заражении виртуальной машины McAfee ePO получает данные о событии с подробной информацией о зараженной виртуальной машине.

Мультигипервизор — стандарты и удобство

В случае использования многоплатформенной версии агент McAfee MOVE AntiVirus — размещенный в конечных точках легковесный компонент — устанавливает связь с сервером сканирования Offload Scan Server, осуществляя координацию антивирусной защиты «от лица» каждой виртуальной рабочей станции. Управление политиками и функциями сканирования выполняются агентом программного обеспечения McAfee ePO. Вы также можете назначить «золотой образ» и выполнить его сканирование, чтобы потом использовать его в качестве «чистого» эталонного образа. Это дает администратору возможность автоматически заполнять глобальные кэши «чистыми» образами для обеспечения более высокой скорости загрузки виртуальных рабочих столов.

Когда пользователь осуществляет доступ к файлу, сервер сканирования McAfee MOVE Offload Scan Server сканирует этот файл и посылает свой ответ виртуальной машине. При обнаружении проблем пользователь получает уведомление в виде всплывающего предупреждения, а файлы помещаются в карантин до принятия решения о дальнейших действиях. Каждую виртуальную машину можно настроить с помощью индивидуальных, уникальных политик, задаваемых в консоли McAfee ePO. Кроме того, есть возможность управлять несколькими виртуальными машинами, объединенными в группу.

Дополнительная информация

Решения McAfee дадут вам тот уровень защиты, который вам нужен, и тот уровень гибкости, который вы заслуживаете. См. **www.mcafee.com/ru/products/data-center-security-suite-for-vdi.aspx**.

Функция	Назначение
Безопасность систем виртуализации	• Повышение уровня защиты рабочих нагрузок, развернутых на инфраструктурах виртуальных рабочих столов, без снижения быстродействия и эффективности использования ресурсов • Мультигипервизорный и безагентный варианты развертывания: развертывание в смешанных средах, в которых используются гипервизоры разных производителей (VMware, Citrix, Hyper-V) • Безагентное развертывание, оптимизированное под VMware, позволяющее повысить уровень быстродействия и плотность виртуальных машин; отсутствие необходимости устанавливать/обновлять агенты McAfee на каждом виртуальном рабочем столе, что упрощает весь процесс и делает его намного более удобным
Базовая защита конечных точек	• Средство антивирусной защиты для физических серверов, занявшее первое место в проведенном компанией NSS Labs тестировании продуктов для защиты от средств использования уязвимостей «нулевого дня» и от попыток обхода защиты • Предотвращение вторжения на узел, обеспечивающее защиту от сложных угроз безопасности, которые в противном случае могут случайно или преднамеренно попасть в организацию • Решение McAfee SiteAdvisor® Enterprise, пресекающее попытки пользователей взаимодействовать с опасными веб-сайтами и дающее возможность ограничивать доступ к потенциально вредоносным веб-сайтам, обеспечивая тем самым соблюдение политик
Белые списки приложений	• Значительно меньшее влияние на быстродействие узла по сравнению с традиционными решениями для защиты конечных точек • Защита от угроз «нулевого дня» и сложных постоянных угроз (advanced persistent threats — APT) без обновления сигнатур, что значительно сокращает время, необходимое для обеспечения защиты • Динамический белые списки, требующие меньших эксплуатационных издержек по сравнению с прежними методами на основе белых списков
Полный сбор информации о виртуальных машинах в частном «облаке»	• Автоматическое обнаружение виртуальных машин в частном «облаке» (VMware vSphere)
Защита файлов и съемных носителей (шифрование)	• Значительное снижение уровня сложности и риска развертывания шифрования благодаря средствам защиты файлов и съемных носителей • Оптимизированная реализация технологии Intel AES-NI, позволяющая обеспечить почти стопроцентное быстродействие на зашифрованных узлах • Автоматическое и незаметное шифрование файлов/папок и съемных носителей (USB-накопителей, компакт-дисков, DVD-дисков) в соответствии с политиками безопасности • Возможность шифровать съемные USB-накопители и безопасно передавать информацию • Защищенный доступ к данным на общих сетевых ресурсах
Централизованное управление с помощью программного обеспечения McAfee ePO	• Централизованное управление физическими и виртуальными системами, включая системы, расположенные в «облаке» (как в частном, так и в публичном), позволяющее собирать больше информации о степени защищенности систем • Упрощение операционных процессов и сокращение временных затрат административного персонала • Снижение затрат на оборудование благодаря сокращению количества необходимых серверов

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com