McAfee Security Suite for Virtual Desktop Infrastructure

Безопасность, в которой вы нуждаетесь, при минимальном снижении быстродействия

В настоящее время наблюдается переход на использование виртуальных рабочих станций. Однако в используемые для этого решения должны быть с самого начала встроены надежные средства защиты. Только так предприятия смогут защитить себя от угроз, не опасаясь снизить уровень быстродействия и сохраняя при этом необходимую плотность серверов. Традиционные антивирусные программы не очень хорошо интегрируются в виртуальную инфраструктуру. Как справиться с этой проблемой? С помощью комплекта McAfee® Security Suite for Virtual Desktop Infrastructure (VDI), который обеспечивает комплексную защиту, оптимизированную для виртуальных рабочих столов.

McAfee Security Suite for VDI обеспечивает защиту от вредоносных программ, оптимизированную для виртуальных рабочих столов, дает возможность использовать белые списки для отражения угроз «нулевого дня» и защищает от вторжений на рабочие столы и утечки данных. Комплект 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 AntiVirus (McAfee MOVE AntiVirus) перераспределяет операции сканирования файлов,

Ключевые преимущества

- Предлагает функции сбора информации и обнаружения рабочих нагрузок за счет McAfee ePO и Cloud Workload Discovery.
- Обеспечивает доступ к уникальному сочетанию черных списков и белых списков для защиты виртуальных рабочих станций от вредоносных программ.
- Оптимизированная защита виртуальных сред, отличающаяся минимальным снижением уровня быстродействия.
- Дополнительные средства защиты от вторжений и веб-атак: 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.

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.

Управление с помощью настраиваемых политик

Программная консоль McAfee® ePolicy Orchestrator® (McAfee ePO™) дает возможность настраивать политики и элементы управления, позволяющие управлять McAfee MOVE AntiVirus. Данные с виртуальных рабочих станций могут быть объединены с данными других систем в рамках единых панелей мониторинга и отчетов. С помощью Cloud Workload Discovery для частного облака 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.

Безагентная версия для VMware

В целях повышения эффективности в McAfee MOVE AntiVirus используется VMware NSX или VMware vCNS. В случае безагентного развертывания эти компоненты используют гипервизор в качестве высокоскоростного соединения, позволяя виртуальной машине безопасности (Security Virtual Machine, SVM) продукта McAfee MOVE AntiVirus выполнять сканирование виртуальных машин, находясь за пределами гостевого образа. В ходе сканирования VMware NSX или VMware vCNS по указанию SVM отправляет в кэш доброкачественные файлы и удаляет или блокирует вредоносные файлы, либо помещает эти файлы в карантин.

После установки и настройки SVM компании VMware, компонентов VMware NSX или VMware vCNS на серверах VMware ESX и драйверов конечных точек VMware NSX или VMware vCNS на гостевых виртуальных машинах, обеспечивается автоматическая защита каждого образа, а значит снимается необходимость устанавливать наше ПО 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 SVM гарантирует их непрерывную защиту на целевом узле без замедления сканирования и без нарушений в работе пользователей.

Интеграция решений McAfee MOVE AntiVirus с vCNS позволяет просматривать состояние виртуального устройства SVM в VMware vCenter

Ключевые преимущества (продолжение)

- Предлагает безагентный и многоплатформенный варианты развертывания.
- Поддерживает гибкую балансировку нагрузки на автономные сканеры для увеличения их производительности по требованию (многоплатформенная версия).
- Интегрировано с механизмом сбора локальной информации о репутации с целью ускорить реагирование на угрозы (многоплатформенная версия).

и получать предупреждения в случае потери связи с SVM. А в случае заражения виртуальной машины McAfee ePO получает данные о событии с подробной информацией о том, какая виртуальная машина заражена. Глубокая интеграция с NSX позволяет синхронизировать политики, созданные в McAfee ePO и правила, назначенные в VMware NSX. Функция присваивания меток уязвимым машинам, не имеющим защиты от вредоносных программ, или машинам, на которых обнаружены вредоносные программы, позволяет мгновенно блокировать виртуальные машины с помощью брандмауэра VMware NSX.

Многоплатформенная версия для всех гипервизоров

В случае использования многоплатформенной версии агент McAfee MOVE AntiVirus — размещенный в конечных точках легковесный компонент — устанавливает связь с сервером сканирования McAfee MOVE 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.

При многоплатформенном развертывании в случае увеличения или уменьшения рабочей нагрузки машины SVM могут автоматически добавляться в пул ресурсов или удаляться из него, повышая или понижая производительность, что обеспечивает неограниченное масштабирование и эффективное использование ресурсов. Уведомления о событиях помогают администраторам понимать специфику текущего использования машин SVM для оптимизации управления ресурсами.

Многоплатформенные версии McAfee MOVE AntiVirus могут дополнять глобальную информацию о репутации, получаемую от McAfee Global Threat Intelligence, локальными данными, предоставляемыми модулем McAfee Threat Intelligence Exchange. Этот модуль предоставляется за отдельную плату и позволяет мгновенно обнаруживать и устранять уникальные вредоносные программы, количество которых постоянно растет. Взаимодействие

Конфигурация McAfee Security Suite for VDI

- McAfee MOVE AntiVirus
  - Многоплатформенное развертывание
  - Безагентное развертывание
- Cloud Workload Discovery для обнаружения рабочих нагрузок в частных облаках (VMware и OpenStack)
- McAfee VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention for Desktop
- McAfee Application Control for Desktops
- McAfee SiteAdvisor® Enterprise (технология)
- McAfee ePolicy Orchestrator

McAfee Threat Intelligence Exchange и McAfee MOVE AntiVirus с McAfee Advanced Threat Defense позволяет динамически анализировать поведение неизвестных приложений в изолированной среде («песочнице») и автоматически обеспечивать невосприимчивость всех виртуальных рабочих станций к недавно обнаруженным вредоносным программам.

Функция	Назначение
Безопасность систем виртуализации	▪ Повышение уровня защиты рабочих нагрузок, развернутых на инфраструктурах виртуальных рабочих столов, достигается без снижения быстродействия и эффективности использования ресурсов. ▪ Безагентное развертывание, оптимизированное под VMware, позволяет повысить уровень быстродействия и плотность виртуальных машин. Отсутствие необходимости устанавливать/обновлять наши агенты на каждом виртуальном рабочем столе позволяет упростить весь процесс и повысить удобство работы. ▪ Многоплатформенное развертывание для всех гипервизоров поддерживает гибкую балансировку нагрузки на автономные сканеры, тем самым увеличивая их производительность по требованию. Оно использует локальную информацию о репутации, позволяя быстрее реагировать на угрозы.
Базовая защита конечных точек	▪ Антивирусная защита McAfee быстрее выполняет сканирование, использует меньший объем памяти, расходует меньше циклов ЦП и защищает лучше, чем любой из существующих продуктов. ▪ Функция предотвращения вторжения на узел обеспечивает защиту от сложных угроз безопасности, которые в противном случае могут случайно или преднамеренно попасть в организацию. ▪ Решение McAfee SiteAdvisor® Enterprise пресекает попытки пользователей взаимодействовать с опасными веб-сайтами и дает возможность ограничивать доступ к потенциально вредоносным веб-сайтам, обеспечивая тем самым соблюдение политик.
Белые списки приложений	▪ Функция значительно уменьшает влияние на быстродействие узла по сравнению с традиционными решениями для защиты конечных точек. ▪ Защищает от угроз «нулевого дня» и сложных постоянных угроз (advanced persistent threats — APT) без необходимости обновлять сигнатуры, что значительно сокращает время, необходимое для обеспечения защиты. ▪ Динамические белые списки требуют меньших эксплуатационных издержек по сравнению с прежними методами на основе белых списков.
Cloud Workload Discovery	▪ Функция обеспечивает полный сбор информации о рабочих нагрузках в облаке и их распределении по платформам, что позволяет идентифицировать слабые места в системе средств защиты.

Функция	Назначение
Защита файлов и съемных носителей (шифрование)	▪ Благодаря средствам защиты файлов и съемных носителей значительно снижается сложность и риск развертывания систем шифрования. ▪ Оптимизированная реализация технологии Intel® AES-NI обеспечивает почти стопроцентное быстродействие на зашифрованных узлах. ▪ Функция обеспечивает автоматическое и незаметное шифрование файлов/папок и съемных носителей (USB-накопителей, компакт-дисков, DVD-дисков) в соответствии с политиками безопасности. ▪ Позволяет шифровать съемные USB-накопители и безопасно передавать информацию. ▪ Предоставляет защищенный доступ к данным на общих сетевых ресурсах.
Централизованное управление с помощью программного обеспечения McAfee ePO	▪ Функция обеспечивает централизованное управление развертываниями в физических, виртуальных и облачных средах, призванное улучшить контроль над средствами защиты, включая управление политиками, развертывание, сбор информации и управление безопасностью на всех платформах. ▪ Упрощает операционные процессы и сокращает трудозатраты административного персонала. ▪ Снижает затраты на оборудование благодаря сокращению количества необходимых серверов.

Дополнительная информация

Решения McAfee дадут вам тот уровень защиты, который вам нужен, с минимальным воздействием на производительность систем. См. **www.mcafee.com/ru/products/data-center-security-suite-for-vdi.aspx**.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru