McAfee Management for Optimized Virtual Environments AntiVirus

Защита вашего частного облака без ущерба для быстродействия

Традиционные антивирусные программы не очень хорошо интегрируются в виртуальную инфраструктуру. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) — оптимизированный, усовершенствованный продукт для защиты ваших виртуальных рабочих станций и серверов от вредоносных программ. Это эффективное решение, существующее в двух версиях: в многоплатформенной версии, предназначенной для большого количества гипервизоров, и в безагентной версии, предназначенной для платформ VMware NSX или VMware vCNS. В обоих случаях вы получаете высочайший уровень защиты, обеспечивающий мгновенное обнаружение и сдерживание угроз, с минимальной нагрузкой на производительность виртуальных машин. McAfee MOVE AntiVirus представляет собой средство защиты от вредоносного ПО, оптимизированное под виртуальные развертывания. Решение позволяет высвободить ресурсы гипервизоров и при этом обеспечить регулярное сканирование виртуальных машин с использованием актуальных сигнатур в соответствии с политикой безопасности.

Оптимизированное управление сканированием

Динамический характер гостевых рабочих станций и виртуальных серверов требует осторожного подхода. На момент инициирования пользовательского сеанса в образах не должно быть вредоносных программ. Это сложная задача, поскольку пользователи часто начинают работать в группах, вызывая 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 MOVE AntiVirus перераспределяет операции сканирования файлов, настройки защиты и обновления DAT-файлов с отдельных гостевых образов на сервер

Ключевые преимущества

- **Балансирует нагрузку при сканировании на наличие вредоносных программ.** Мгновенная защита с низкой нагрузкой на память и ЦП.
- **Предотвращает «антивирусные штормы».** Сканирование при обращении и сканирование по запросу.
- **Предлагает гибкие варианты развертывания:** многоплатформенную версию (все основные гипервизоры, виртуальные машины Windows) или безагентный вариант (виртуальные машины VMware, Windows и Linux).
- **Оптимизирует использование ресурсов:** гибкая балансировка нагрузки на автономные сканеры с уведомлениями о событиях (многоплатформенная версия).

сканирования с оптимизацией нагрузки (Offload Scan Server). Мы создаем и обслуживаем глобальный кэш сканированных файлов, что означает, что после сканирования файла и подтверждения отсутствия в нем вредоносного кода другим виртуальным машинам при доступе к этому файлу уже не придется ожидать результатов сканирования. Таким образом снижаются выделенные на каждую виртуальную машину ресурсы памяти, что увеличивает общий объем свободных ресурсов и повышает эффективность их использования.

McAfee MOVE AntiVirus позволяет устанавливать разные политики для сканирования при доступе и сканирования по требованию, что дает возможность для тонкой настройки функций безопасности. Например, основываясь на разумной оценке риска в реальном времени, администраторы могут установить сканирование по доступу, чтобы избежать падения производительности, а позднее, когда влияние на производительность не так высоко, использовать сканирование по требованию с более жесткими политиками.

Полный сбор информации во всех облаках

Неудовлетворительный сбор информации затрудняет применение надлежащих политик безопасности для виртуализированных сред. Решение McAfee Cloud Workload Discovery для частного облака, включая среды VMware и OpenStack, обеспечивает полный сбор информации о происходящем в виртуальных центрах обработки данных и передает на консоль McAfee ePO такие ключевые характеристики, как серверы, гипервизоры и виртуальные машины. Если администратор получает информацию о состоянии защиты всех виртуальных машин и может отслеживать отношения «гипервизор–виртуальная машина» в режиме почти реального времени, то обеспечение безопасности виртуального ЦОД значительно упрощается. Настраиваемая, дающая визуальное представление панель мониторинга отображает состояние сканирования безопасности, краткие общие обзоры и архивные данные состояния защиты активов.

Комплекты McAfee Server Security Suite Essentials и McAfee Server Security Suite Advanced позволяют собирать информацию и контролировать происходящее в публичных облаках и на физических серверах Amazon Web Services (AWS) и Microsoft Azure.

Управление с помощью настраиваемых политик

Для конфигурирования политик и средств контроля McAfee MOVE AntiVirus используется уже знакомая вам программная консоль McAfee ePO. Вы можете комбинировать виртуальные данные с данными вашей физической системы и публичного облака для унификации панелей и отчетов. С помощью McAfee Cloud Workload Discovery администраторы могут создавать индивидуальные политики для виртуальной машины, кластера или центра обработки данных в соответствии с требованиями обеспечения защиты конкретного центра обработки данных.

Ключевые преимущества (продолжение)

- **Блокирует неизвестные угрозы и угрозы «нулевого дня» в течение нескольких секунд:** локальный сбор информации о репутации сочетается с анализом поведения «в песочнице» (многоплатформенная версия, дополнительный модуль — предоставляется за отдельную плату).
- **В решении используется консоль McAfee® ePolicy Orchestrator® (McAfee ePO™)** для полного сбора информации и управления физическими, виртуальными и облачными развертываниями.

Дополнительные функции McAfee MOVE AntiVirus

Управление и сбор информации:

- возможность мгновенно запланировать сканирование по требованию для виртуальной машины или для группы виртуальных машин;
- повышенная точность сканирования с целенаправленным сканированием по требованию;
- автоматическое развертывание сканера с оптимизацией нагрузки на каждом гипервизоре благодаря интеграции с VMware NSX Service Composer;
- полный контроль за всеми событиями благодаря панелям, отчетам и предупреждениям, рассылаемым по электронной почте.

Упрощенное развертывание и настройка:

- развертывание и настройка сканера с оптимизацией нагрузки на нескольких гипервизорах (безагентная версия);
- восстановление помещенных в карантин файлов с помощью консоли McAfee ePO (многоплатформенная версия);
- подробная диагностика для настройки производительности антивирусной защиты;
- автоматическое управление политиками при безагентном и многоплатформенном вариантах развертывания.

Безагентная версия для сред VMware

McAfee MOVE AntiVirus использует VMware NSX или VMware vCNS для повышения эффективности работы. В случае безагентного развертывания эти компоненты используют гипервизор в качестве высокоскоростного соединения, позволяя специализированной виртуальной машине (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 машины SVM, 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 без необходимости устанавливать ПО 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 машина SVM гарантирует их непрерывную защиту на целевом узле без замедления сканирования и без нарушений в работе пользователей.

Интеграция продуктов McAfee с VMware vCNS позволяет просматривать состояние машины SVM в vCenter и получать предупреждения в случае потери

Конфигурации McAfee MOVE AntiVirus

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus:
  - Многоплатформенное развертывание
  - Безагентное развертывание
- Cloud Workload Discovery для обнаружения рабочих нагрузок в частных облаках (VMware и OpenStack)
- McAfee ePO (ПО)

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus:
  - Многоплатформенное развертывание
  - Безагентное развертывание
- Cloud Workload Discovery для обнаружения рабочих нагрузок в частных облаках (включая VMware и OpenStack)
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- Защита памяти и защита веб-приложений
- McAfee ePO (ПО)

связи с SVM. А в случае заражения виртуальной машины консоль McAfee ePO получает данные о событии с подробной информацией о том, какая виртуальная машина заражена. Глубокая интеграция с VMware NSX позволяет синхронизировать политики, созданные в консоли 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.

Развертывание безагентного варианта McAfee MOVE AntiVirus с одновременной поддержкой VMware vCNS и VMware NSX позволяет клиентам VMware vCNS очень без труда автоматически перейти на использование VMware NSX.

Многоплатформенная версия для всех основных гипервизоров

В случае использования многоплатформенной версии, включая vSphere, Hyper-V, KVM и XenServer, агент McAfee MOVE AntiVirus — размещенный в конечных точках легковесный компонент — устанавливает связь с машиной SVM, осуществляя координацию антивирусной защиты «от лица» каждой виртуальной машины. Поддержка локального кэша, управление политиками и функциями сканирования выполняются агентом программного обеспечения McAfee MOVE AntiVirus. Вы можете назначить «золотой образ» и выполнить его сканирование, чтобы потом использовать его в качестве «чистого» эталонного образа. Предварительное заполнение локального кэша «чистыми» эталонными образами позволяет добиться максимальной скорости загрузки виртуальных машин.

При обращении к файлу McAfee MOVE Offload Scan Server сканирует этот файл и возвращает результат на виртуальную машину. При обнаружении проблем пользователь получает уведомление в виде всплывающего предупреждения. Затем пользователь может удалить вредоносные файлы, запретить к ним доступ или поместить их в карантин.

При колебании потребностей в сканировании при многоплатформенном развертывании 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 (McAfee GTI), локальными данными, предоставляемыми модулем McAfee Threat Intelligence Exchange. Этот модуль предлагается за отдельную плату и позволяет мгновенно обнаруживать и устранять уникальные вредоносные программы, количество которых постоянно растет.

Взаимодействие 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 конечных точек к недавно обнаруженным вредоносным программам. Интеграция McAfee MOVE AntiVirus с McAfee Network Security Platform посредством McAfee Threat Intelligence Exchange позволяет реализовать принцип многоуровневой безопасности, обеспечивающий комплексную защиту периметра и виртуальных машин.

Комплексное управление политиками для безагентного и многоплатформенного вариантов

Многие организации захотят воспользоваться возможностью поддержки McAfee MOVE AntiVirus как безагентного, так и многоплатформенного развертываний. McAfee MOVE AntiVirus дает администраторам систем безопасности возможность задавать политики безопасности и последовательно управлять ими с помощью одной точки расширения консоли McAfee ePO, обеспечивая простое и автоматическое управление столь разными методами.

Дополнительная информация

Решения McAfee дадут вам тот уровень защиты, который вам нужен, и тот уровень гибкости, который вы заслуживаете.

Для получения дополнительной информации посетите веб-страницу **www.mcafee.com/ru/products/move-anti-virus.aspx**.

Архитектура	Многоплатформенное развертывание	Безагентное развертывание
Поддержка гипервизора/платформы	Все основные гипервизоры, включая VMware, Citrix, Hyper-V и KVM	VMware
Платформа сканирования	Windows 2008, Windows 2012 R2, Windows Server 2016	Linux Ubuntu 16.04
Масштабируемость развертывания	Одна специализированная виртуальная машина (Security Virtual Machine, SVM) способна обеспечивать защиту виртуальных машин с различных гипервизоров; возможность гибкой инициализации машин SVM	Одна машина SVM на один узел ESX
Связь с виртуальными машинами	Через сеть	Через гипервизор
Защита виртуальных машин	Windows	Windows и Linux

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