McAfee Management for Optimized Virtual Environments AntiVirus

Теперь у вас есть тот уровень защиты, который вам нужен, и тот уровень гибкости, который вы заслуживаете.

Ключевые преимущества

Балансировка нагрузки при сканировании на наличие вредоносных программ
- Мгновенная защита с низкой нагрузкой на память и ЦП

Предотвращение «антивирусных штормов»
- Сканирование при обращении и сканирование по графику

Гибкость развертывания
- Многоплатформенное (без привязки к одному поставщику) или безагентное для платформы VMware

Минимум настроек и обновлений
- Специализированное отказоустойчивое виртуальное устройство

Блокирование неизвестных угроз и угроз «нулевого дня»
- Анализ файлов в реальном времени с помощью технологии McAfee Global Threat Intelligence

Использование ПО McAfee ePO
- Визуальное представление данных, визуальный контроль и средства создания визуальных отчетов по всем конечным точкам

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 платформ разных производителей, и в безагентной версии, предназначенной для платформы VMware vShield. Обе эти версии обеспечивают одинаково гибкую защиту высшего класса и одинаково высокий уровень быстродействия.

Решение McAfee MOVE AntiVirus, входящее в линейку продуктов Intel® Security, обеспечивает защиту от вредоносных программ, оптимизированную с учетом ресурсных ограничений виртуальных сред. McAfee MOVE AntiVirus высвобождает ресурсы гипервизоров, гарантируя при этом регулярное выполнение проверок безопасности в соответствии с политикой организации.

Оптимизированная архитектура сканирования

Динамический характер гостевых рабочих станций и виртуальных серверов требует осторожного подхода. На момент инициирования пользовательского сеанса в образах не должно быть вредоносных программ. 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 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, 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. 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.

Полный контроль над процессами в центре обработки данных

Получение полного контроля над процессами во всей виртуальной среде центра обработки данных может представлять собой непростую задачу для администраторов системы защиты. McAfee Data Center Connector for VMware vSphere обеспечивает полное представление о виртуальных центрах обработки данных и заполняет консоль McAfee ePolicy Orchestrator® (McAfee ePO™) данными об основных системах, таких как серверы, гипервизоры, виртуальные машины и даже «облако». Клиенты могут обнаруживать и просматривать все виртуальные машины независимо от того, развернуты на них средства защиты McAfee или нет. Благодаря возможности получать полную информацию о центрах обработки данных упрощается задача обеспечения их защиты. Администраторы могут отслеживать отношения «гипервизор-виртуальная машина», состояние защиты и состояние питания практически в режиме реального времени. Настраиваемая, дающая быстрое визуальное представление панель мониторинга отображает состояние сканирования безопасности, краткие общие обзоры, архивные данные состояния защиты активов. В McAfee Server Security Suite Essentials и McAfee Server Security Suite Advanced включены дополнительные соединительные модули для центров обработки данных (Data Center Connector), позволяющие использовать этот функционал при работе с общедоступным «облаком» Amazon AWS, «облаком» Microsoft Azure и «облаками» на базе OpenStack.

intel Security

Конфигурации McAfee MOVE AntiVirus

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus
  - Многоплатформенное развертывание
  - Безагентное развертывание
- McAfee MOVE AntiVirus Scheduler
- McAfee Data Center Connector for vSphere
- McAfee ePolicy Orchestrator (ПО)

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus
  - Многоплатформенное развертывание
  - Безагентное развертывание
- McAfee MOVE AntiVirus Scheduler
- McAfee Data Center Connector for vSphere
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise (ПО)
- McAfee Desktop Firewall, защита памяти и защита веб-приложений
- McAfee ePolicy Orchestrator (ПО)

Управление с помощью настраиваемых политик

Для конфигурирования политик и средств контроля McAfee MOVE AntiVirus используется уже знакомая вам программная консоль McAfee ePO. Она позволяет объединять данные с виртуальных рабочих станций с данными физических систем в рамках единых панелей мониторинга и отчетов. С помощью McAfee Data Center Connector администраторы могут создавать индивидуальные политики для виртуальной машины, кластера или центра обработки данных в соответствии с требованиями обеспечения защиты конкретного центра обработки данных.

Дополнительные функции McAfee MOVE AntiVirus

Управление и сбор информации:

- возможность мгновенно запланировать сканирование по требованию на виртуальной машине или на группе виртуальных машин;
- автоматическое развертывание виртуального защитного устройства (SVA) на каждом гипервизоре благодаря интеграции с VMware NSX Service Composer;
- улучшенный модуль Data Center Connector для VMware vCenter.

Упрощенное развертывание и настройка:

- развертывание и настройка SVA на нескольких гипервизорах (безагентный вариант);
- восстановление файлов, помещенных в карантин, из консоли McAfee ePO (многоплатформенный вариант);
- улучшенные методы диагностики для настройки быстродействия антивируса.

Более эффективная оптимизация ресурсов:

- гибкие политики настройки (многоплатформенный вариант).

Безагентный вариант для сред VMware

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

Установив и настроив 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 ваши виртуальные машины с одного узла на другой, и при этом 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 в случае заражении виртуальной машины McAfee ePO получает данные о событии с подробной информацией о том, какая виртуальная машина заражена.

Многоплатформенное решение обеспечивает стандарты и удобство

В случае использования многоплатформенной версии агент McAfee MOVE AntiVirus — размещенный в конечных точках легковесный компонент — устанавливает связь с сервером сканирования, осуществляя координацию антивирусной защиты «от лица» каждой виртуальной рабочей станции. Управление политиками и функции сканирования выполняются агентом McAfee Agent. 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 выделенный сервер сканирования McAfee MOVE AntiVirus 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.

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	VMware, Citrix, Hyper-V	Только VMware
Платформа сканирования	Windows Server 2008, Windows Server 2012 R2	Linux Ubuntu 12.4
Масштабируемость развертывания	Один выделенный сервер сканирования способен обеспечивать защиту виртуальных машин с большого числа разных гипервизоров	Одно устройство Security Virtual Appliance на узел с ESX
Связь с виртуальными машинами	Через сеть	Через гипервизор

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