McAfee Server Security

Оптимизация системы безопасности. Минимизация потерь быстродействия.

Гибридные облака отличаются уникальными требованиями к безопасности, которые невозможно выполнить с помощью прежних решений. Поскольку традиционные средства защиты позволяют собирать лишь ограниченные данные о происходящем в облачной инфраструктуре, как вы собираетесь защищать то, чего не видите? Приходится ли вам жертвовать безопасностью ради получения динамичной децентрализованной облачной инфраструктуры с поддержкой DevOps? Или вам приходится выбирать между защитой своих виртуальных серверов и оптимизацией их быстродействия? Если вы выберете защиту, вы обеспечите высокий уровень доступности, защитите свои данные и на «ура» пройдете очередной аудит нормативно-правового соответствия! Если вы выберете быстродействие, то сможете поднять уровень отдачи от своих инвестиций в технологии, не говоря уже о похвале со стороны финансового директора. Так что же вы выберете: защиту или динамичность или быстродействие?

Ключевые преимущества

- Мгновенное обнаружение рабочих нагрузок и установление контроля над ними для обеспечения систематической и непрерывной защиты физических, виртуальных и облачных развертываний.
- Защита серверов и облачных рабочих нагрузок от все более изощренных угроз сегодняшнего дня при минимальном снижением быстродействия и с возможностью масштабирования по требованию в динамических облачных средах.
- McAfee Server Security Suite Essentials включает в себя обязательные средства защиты облачных нагрузок и серверов: оптимизированный антивирус для виртуальных сред, средства предотвращения вторжений и др.
- McAfee Server Security Suite Advanced — наш самый полнофункциональный комплект средств защиты, включающий в себя функции проверки по белым спискам и контроля за изменениями.

На стыке традиционных средств безопасности и требований защиты облака

Задача обеспечения безопасности современных облачных сред с помощью устаревших средств защиты заставляет многих директоров ИТ-подразделений принимать именно такое решение. Средства защиты должны быть такими же гибкими, как и динамические облака, позволяющие увеличивать или сокращать количество рабочих нагрузок по требованию. Традиционные средства защиты по своей природе слишком статичны и не могут справиться с этой задачей, что приводит к появлению огромных брешей в облачной защите. Столкнувшись с высокой нагрузкой на ЦП при использовании обычных средств защиты физических серверов на виртуальных системах или с высокими расходами на администрирование при использовании разрозненных специализированных решений без центрального интерфейса управления, многие ИТ-администраторы просто отключили свои средства защиты конечных точек и полностью положились на средства защиты периметра.

Сложные требования, предъявляемые к современным средствам защиты серверов

Конечно, на критически важных облачных серверах необходимо обязательно устанавливать средства обеспечения безопасности, иначе произойдет катастрофа. Но дело в том, что устаревшие технологии обеспечения безопасности были разработаны для защиты выделенных физических систем. Они не успевают за темпами развития технологий виртуализации и не соответствуют требованиям современных смешанных сред ЦОД. В настоящее время существует острая потребность в таких решениях для защиты серверов и облачных рабочих нагрузок, которые:

- поддерживают сбор информации об облачной инфраструктуре и автоматически масштабируются в соответствии с динамикой облачных рабочих нагрузок;
- обеспечивают оптимизированную защиту, специально разработанную с целью снизить воздействие на быстродействие виртуальных сред;
- позволяют управлять всеми элементами системы безопасности в масштабах всей серверной среды, включающей в себя физические, виртуальные и облачные развертывания, с помощью единой консоли управления.

Комплекты McAfee Server Security

McAfee® Server Security Suite Essentials включает в себя обязательные средства защиты облачных нагрузок и серверов: оптимизированный антивирус, средства предотвращения вторжений и др. McAfee® Server Security Suite Advanced — самый комплексный набор средств защиты облачных рабочих нагрузок и серверов, дополнительно включающий в себя расширенный функционал белых списков для защиты от угроз «нулевого дня» и средства контроля за изменениями для обеспечения нормативно-правового соответствия.

McAfee Server Security Suite Essentials	McAfee Server Security Suite Advanced
Консоль McAfee ePolicy Orchestrator® (McAfee ePO™)	Консоль McAfee ePO
Функция Cloud Workload Discovery для обнаружения рабочих нагрузок в гибридных облачных средах	Функция Cloud Workload Discovery для обнаружения рабочих нагрузок в гибридных облачных средах
Защита от вредоносных программ (оптимизирована для виртуальных машин)	Защита от вредоносных программ (оптимизирована для виртуальных машин)
Брандмауэр	Брандмауэр
Предотвращение вторжений на узел	Предотвращение вторжений на узел
	Белые списки приложений
	Мониторинг целостности файлов

Сбор информации об облачной инфраструктуре

Функция Cloud Workload Discovery для обнаружения рабочих нагрузок в гибридном облаке — одна из основных функций McAfee Server Security Suite Advanced и McAfee Server Security Suite Essentials — позволяет значительно облегчить задачу выявления брешей в защите постоянно расширяющегося гибридного центра обработки данных. Функция Cloud Workload Discovery для обнаружения рабочих нагрузок в гибридных облаках, созданных с помощью VMware, OpenStack, AWS или Microsoft Azure, обеспечивает полный сбор информации обо всех рабочих нагрузках и лежащих в их основе платформах. Возможность обнаруживать ненадежные средства защиты, небезопасные настройки брандмауэров и средств шифрования, а также признаки взлома, такие как, например, подозрительный трафик, позволяет повысить скорость выявления угроз. А для быстрого устранения выявленных угроз можно использовать программное обеспечение McAfee ePO или средства DevOps.

Оптимизированная защита для виртуальных сред

McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) — оптимизированный, усовершенствованный продукт для защиты ваших виртуальных рабочих станций и серверов от вредоносных программ, избавляющий вас от необходимости жертвовать безопасностью ради быстродействия. 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 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.

Автоматическое масштабирование

Использование наших средств защиты серверов и гибридных облаков позволяет динамическим облачным средам, поддерживающим DevOps,

оставаться динамическими без ущерба для безопасности. Способность средств защиты гибко масштабироваться в соответствии с динамикой облачных рабочих нагрузок позволяет обеспечить непрерывность защиты. Благодаря гибкому механизму развертывания защиты в частных облаках McAfee MOVE AntiVirus может по мере необходимости автоматически изменять количество автономных серверов сканирования в пуле ресурсов (добавляя или убирая их). В случае рабочих нагрузок в AWS и Azure у пользователей есть возможность настроить защиту на уровне шаблонов, чтобы она автоматически масштабировалась при увеличении или сокращении количества рабочих нагрузок.

Централизованное управление

Программное обеспечение McAfee ePO обеспечивает централизованное управление физическими и виртуальными серверами, в том числе расположенными в частных и общедоступных облаках. Управляя всей своей инфраструктурой конечных точек из единой консоли, вы обеспечите более надежную и более согласованную защиту от угроз безопасности и снизите совокупную стоимость владения своей инфраструктурой. Все компоненты комплекта тесно интегрированы с платформой управления безопасностью McAfee ePO, что обеспечивает эффективный централизованный подход к оценке рисков, управлению безопасностью и реагированию на инциденты.

Рис. 1. Единая система управления решениями McAfee во всех облаках и на всех серверах.

Успех комплектов для защиты серверов

Комплекты McAfee Server Security представляют собой первое в отрасли комплексное решение для обеспечения безопасности критически важных служб в современных смешанных физических и виртуальных средах. В них используется сочетание технологий защиты серверов, позволяющее свести к минимуму нагрузку на процессор, иметь полный набор средств управления всеми важнейшими рабочими нагрузками, обеспечить поддержку всех основных сред виртуализации и централизованно управлять средствами защиты с помощью единой административной консоли. За дополнительной информацией обращайтесь на веб-сайт McAfee по адресу **www.mcafee.com/ru/products/data-center-security/server-security.aspx**.

McAfee Together is power.

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