McAfee Server Security Suite Advanced

Комплексный набор средств защиты физических, виртуальных и облачных сред с технологией белых списков и механизмом контроля за изменениями

При отсутствии целостного, всестороннего подхода обеспечение защиты новых серверов и облачных рабочих нагрузок от все более изощренных угроз в современных сложных ИТ-средах становится все более и более трудной задачей. McAfee® Server Security Suite Advanced позволяет обеспечить единообразную и непрерывную защиту во всех физических, виртуальных и публичных облачных развертываниях. Комплексный набор средств защиты включает в себя обязательные средства антивирусной защиты, брандмауэр, средства предотвращения вторжений, технологию белых списков для защиты от угроз «нулевого дня», а также механизм контроля за изменениями, обеспечивающий выполнение нормативно-правовых требований. Передовые средства защиты сводят к минимуму потери быстродействия физических и виртуальных серверов и автоматически масштабируются в соответствии с динамикой облачных рабочих нагрузок.

Мгновенное обнаружение рабочих нагрузок и установление контроля над ними

Функция Cloud Workload Discovery для обнаружения рабочих нагрузок в гибридном облаке — одна из основных функций McAfee Server Security Suite Advanced — 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. Для быстрого устранения выявляемых уязвимостей можно использовать программное обеспечение McAfee® ePolicy Orchestrator® (McAfee ePO™) или средства DevOps.

Ключевые преимущества

- Решение McAfee ePO централизует управление средствами защиты конечных точек, сетей и данных, а также решениями для обеспечения нормативно-правового соответствия, поставляемыми McAfee и другими производителями
- Сбор подробной информации о происходящем, оценка рисков и устранение уязвимостей с помощью функции Cloud Workload Discovery для обнаружения рабочих нагрузок в гибридном облаке
- Защита виртуальных серверов от вредоносных программ благодаря сочетанию технологии черных списков и средств предотвращения вторжений с передовой технологией белых списков и механизмом контроля за изменениями
  - Защита от неизвестных угроз благодаря запрету запуска нежелательных приложений

Использование большого количества разных облачных рабочих нагрузок, имеющих уникальные профили риска и уникальные наборы требований к безопасности, сильно усложняет задачу обеспечения безопасности облака. Cloud Workload Discovery дает возможность оценивать рабочие нагрузки с точки зрения их соответствия политикам, что упрощает задачу сравнения фактического набора используемых средств защиты облачных рабочих нагрузок с тем набором средств защиты, который необходим для обеспечения адекватного уровня защиты и нормативно-правового соответствия. Как только риски безопасности обнаружены, для обеспечения полной защиты необходима всего пара щелчков мышью.

Интеграция Cloud Workload Discovery с консолью управления McAfee ePO дает организациям эффективное средство управления, позволяющее внедрять защитные решения во всех физических, виртуальных и облачных средах. Благодаря этой интеграции администраторы систем безопасности, которым необходимо реагировать на предупреждения об угрозах и обеспечивать принудительное применение политик, могут использовать для этого одну-единственную платформу управления с упрощенными рабочими процессами.

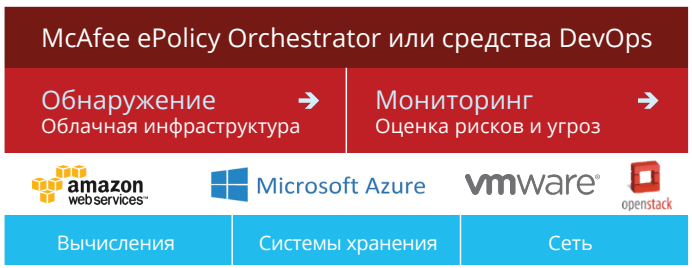

Рис. 1. Cloud Workload Discovery позволяет получить устойчивое преимущество в защите.

Использование McAfee Server Security Suite Advanced 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. Гибкий механизм развертывания защиты в частных облаках позволяет по мере увеличения или сокращения количества рабочих нагрузок автоматически изменять количество 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 по мере изменения рабочих нагрузок.

Комплексная защита

Комплект McAfee Server Security Suite Advanced обеспечивает самую комплексную защиту всех видов серверов — и физических, и виртуальных, и облачных. Кроме того, обеспечиваемая им защита от атак, проводимых методом переполнения буфера на системах под управлением 32-разрядных и 64-разрядных версий Windows, и уникальное сочетание технологий черных списков, белых списков и контроля за изменениями не имеют себе равных в отрасли. Данный комплект включает в себя:

Ключевые преимущества (продолжение)

- Непрерывное выявление изменений системного уровня во всех распределенных и удаленных ресурсах, помогающее выполнять нормативно-правовые требования
- Блокирование неизвестных угроз «нулевого дня» за считанные секунды с помощью локальной информации о репутации, сочетаемой с результатами анализа кода в изолированной среде («песочнице»)
- Оптимизация защиты физических и виртуальных сред при минимальном снижении быстродействия

- **McAfee Application Control for Servers.** Это решение для создания белых списков дает возможность допускать к работе на серверах только разрешенное программное обеспечение и тем самым защитить серверы от неизвестного вредоносного ПО, угроз «нулевого дня» и угроз повышенной сложности. В этом централизованно управляемом решении используется динамическая модель доверия, позволяющая обойтись без трудоемких рабочих процессов управления списками.
- **McAfee Change Control for Servers.** Возможность непрерывно отслеживать изменения системного уровня, вносимые в любой точке распределенной сети, включая удаленные объекты, помогает обеспечить соблюдение законодательных и нормативных требований, таких как закон Сарбейнса-Оксли и Стандарт защиты информации в индустрии платежных карт (PCI DSS).
- **Модуль предотвращения угроз решения McAfee Endpoint Security.** Один из элементов расширяемой архитектуры взаимодействующих между собой решений для защиты серверов под управлением Microsoft Windows и Linux от средств использования уязвимостей «нулевого дня» и атак повышенной сложности.
- **McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus).** Это решение для защиты от вредоносных программ разработано специально для виртуальных сред. Его можно приобрести либо в безагентном варианте, настроенном на VMware NSX и VMware vCNS, либо в многоплатформенном варианте, который можно использовать со всеми основными гипервизорами (Microsoft Hyper-V, VMware, KVM, Xen и др.).
- **McAfee Host Intrusion Prevention for Server.** Это решение обеспечивает защиту компаний от сложных угроз безопасности путем мониторинга поведения кода на серверах и анализа событий на наличие подозрительных действий.
- **Модуль брандмауэра решения McAfee Endpoint Security.** Этот брандмауэр осуществляет мониторинг сетевого трафика и интернет-трафика и осуществляет перехват подозрительных данных.

McAfee Server Security Suite Advanced может дополнять информацию о глобальных угрозах, получаемую из McAfee Global Threat Intelligence (McAfee GTI), данными о локальных угрозах, получаемыми из McAfee Threat Intelligence Exchange (дополнительный модуль, приобретаемый отдельно), что позволяет мгновенно обнаруживать и нейтрализовать уникальные образцы вредоносных программ, количество которых постоянно увеличивается. Взаимодействие McAfee Threat Intelligence Exchange и решений в составе комплекта 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.

В области управления уязвимостями McAfee имеет партнерское соглашение с компанией Rapid7. Разработанное компанией Rapid7 решение Nexpose обнаруживает и приоритизирует уязвимости, а также подтверждает устранение рисков.

Минимальные потери быстродействия

Хотя для большинства компаний безопасность является одним из основных приоритетов, некоторые из них не спешат решать вопрос с защитой серверов из-за опасений возможного снижения быстродействия. McAfee Server Security Suite Advanced позволяет обеспечить защиту физических и виртуальных серверов без снижения их быстродействия даже во время сканирования на наличие вредоносных программ.

В отличие от многих других продуктов для защиты от вредоносных программ McAfee Endpoint Security и McAfee MOVE AntiVirus потребляют незначительное количество вычислительных ресурсов. McAfee Endpoint Security отличается высокой скоростью сканирования, оптимизирует расход ЦП и памяти и обеспечивает более надежную защиту, чем другие продукты для защиты от вредоносных программ. McAfee MOVE AntiVirus освобождает виртуальные машины от необходимости проводить сканирование на наличие вредоносных программ, что позволяет обеспечивать мгновенную защиту при низкой нагрузке на память и ЦП. Наличие отдельных политик для сканирования при доступе и сканирования по требованию позволяет более эффективно контролировать уровни быстродействия и безопасности.

Оптимизация безопасности серверов — этооптимизация бизнеса

Огромный потенциал виртуализации и облачных вычислений может быть в полной мере реализован только при обеспечении достаточного уровня безопасности. Компания McAfee предлагает решения для защиты серверов, масштабируемые по мере роста организации. Предлагаемый нами комплект решений позволяет обеспечивать безопасность серверов и облачных рабочих нагрузок в физических, виртуальных и облачных средах, отличающихся постоянно растущей динамичностью.

Функция	Назначение
Управление из единой консоли	▪ Централизованное управление физическими, виртуальными и облачными развертываниями позволяет повысить эффективность управления защитой (т. е. управления политиками, развертыванием, сбором информации и т. д.) на всех платформах. ▪ Упрощение оперативных аспектов и сокращение временных затрат административного персонала.
Мгновенное обнаружение рабочих нагрузок и установление контроля над ними	▪ Вы сможете обнаруживать физические серверы и иметь полное представление о том, что происходит с вашими рабочими нагрузками и платформами в средах VMware vSphere, OpenStack, AWS и Microsoft Azure. ▪ Непрерывность защиты обеспечивается благодаря автоматической масштабируемости средств защиты в соответствии с динамикой облачных рабочих нагрузок.

Функция	Назначение
Безопасность систем виртуализации	▪ Оптимизированная защита рабочих нагрузок, развернутых в виртуальных инфраструктурах, без снижения быстродействия и эффективности использования ресурсов. ▪ Возможность выбора между многоплатформенным (все основные гипервизоры) и безагентным (VMware NSX и VMware vCNS) вариантами развертывания позволяет обеспечить высокий уровень быстродействия и плотности виртуальных машин.
Защита публичного облака	▪ Вы сможете проводить аудит безопасности платформ, развернутых в AWS и Microsoft Azure, в том числе аудит настроек брандмауэра и средств шифрования. ▪ В случае AWS возможность сбора информации о трафике и сетевых угрозах позволяет обеспечить полную защиту.
Белые списки приложений	▪ Значительно меньшее влияние на быстродействие узла по сравнению с традиционными решениями для защиты серверов. ▪ Обеспечьте защиту от угроз «нулевого дня» и сложных постоянных угроз (advanced persistent threats — APT) без обновления сигнатур, что значительно сокращает время, необходимое для обеспечения защиты. ▪ Использование динамических белых списков позволяет сократить расходы на эксплуатацию решения.
Контроль за изменениями	▪ Предотвращение внесения несанкционированных изменений в критически важные системные файлы, каталоги и настройки, позволяющее администраторам экономить время на устранение нарушений безопасности. ▪ В режиме реального времени решение отслеживает и проверяет каждую попытку внесения изменений на вашем сервере, обеспечивая соблюдение политики изменений по временному интервалу, источнику или уведомлению о разрешении изменений.
Базовая защита серверов	▪ Средства защиты от вредоносных программ обеспечивают защиту от средств использования уязвимостей «нулевого дня» и атак повышенной сложности. ▪ McAfee Host Intrusion Prevention System обеспечивает защиту от сложных угроз безопасности, которые в противном случае могут попасть в организацию либо случайным, либо преднамеренным образом.
Локальный сбор информации о репутации	▪ Интеграция с McAfee Threat Intelligence Exchange (дополнительный модуль, приобретаемый отдельно) позволяет за считанные секунды блокировать неизвестные угрозы «нулевого дня».

Дополнительная информация

За дополнительной информацией о преимуществах McAfee Server Security Suite Advanced обращайтесь по адресу **www.mcafee.com/ru/products/server-security-suite-advanced.aspx**.

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