



McAfee Server Security Suite Advanced

Ключевые преимущества

- Наличие единой централизованной консоли управления, позволяющей обнаруживать все физические и виртуальные серверы, в том числе находящиеся в облаке
- Сочетание белых и черных списков, обеспечивающее защиту физических и виртуальных серверов от вредоносных программ
 - Использование метода динамических белых списков, позволяющее защищать узлы от неизвестных угроз путем запрета запуска нежелательных приложений с помощью McAfee Application Control for Servers
 - Непрерывное выявление изменений системного уровня во всех распределенных и удаленных ресурсах, помогающее выполнять нормативно-правовые требования
- Обеспечение оптимизированной защиты виртуальных сред, отличающейся минимальным снижением уровня быстродействия, с помощью McAfee MOVE AntiVirus

Передовые средства защиты серверов в физических, виртуальных и облачных средах с использованием технологии белых списков

В последние годы в центрах обработки данных наблюдается крупная смена парадигмы: меняются системы хранения, сети, серверы и выполняемые приложения. Многообразие центров обработки данных и быстрый переход к облачным технологиям требуют новых подходов к обеспечению безопасности этих сред. Задача специалистов по корпоративным ИТ и обеспечению безопасности состоит в создании централизованной и надежной системы безопасности для физических, виртуальных и облачных сред, которая будет способствовать повышению уровня динамичности и рентабельности бизнеса. Комплект McAfee® Server Security Suite Advanced, входящий в линейку продуктов Intel® Security, предоставляет собой самый комплексный набор средств защиты серверов и управления ими для физических, виртуальных и облачных сред. Благодаря наличию таких дополнительных функций, как белые списки и контроль за изменениями, он также помогает поддерживать нормативно-правовое соответствие.

Обнаружение любых рабочих нагрузок

Обнаружить в физических, виртуальных и облачных средах все рабочие нагрузки, к которым требуется применить необходимые политики безопасности, зачастую бывает нелегко. В нашем случае простота управления рабочими нагрузками достигается с помощью предоставляемых нами отчетов о сканировании среды, которые дают возможность обнаруживать незащищенные конечные точки и определять уровень их соответствия требованиям безопасности. Благодаря соединительным модулям для программного обеспечения McAfee® ePolicy Orchestrator® (McAfee ePO™) пользователи McAfee Server Security Suite Advanced получают возможность

обнаруживать все физические и виртуальные серверы, включая те, которые находятся в облаке (как в частном, так и в публичном). В комплект входят соединительные модули McAfee Data Center Connector for VMware vSphere, Amazon AWS, OpenStack и Microsoft Azure. Вместе они дают возможность осуществлять мониторинг всех виртуальных машин (как локальных, так и удаленных) и применять к ним детально настраиваемые политики, обеспечивающие надежную защиту. Панели мониторинга позволяют получать информацию о защищенности памяти ОС, о привязке виртуальных машин к гипервизорам, о местонахождении каждой виртуальной машины и т. п.

Ключевые преимущества (продолжение)

- Использование соединительных модулей McAfee Data Center Connector for VMware vSphere, Amazon Web Services, OpenStack и Microsoft Azure, позволяющих собирать полную информацию о статусе защищенности всех виртуальных машин в частном и публичном облаке
- Безагентный резидентный брандмауэр, использующий VMware vCNS App для организации виртуальных машин в безопасные сетевые группы или для их изолирования

Защита серверов

Комплект McAfee Server Security Suite Advanced обеспечивает самую комплексную защиту всех видов серверов — и физических, и виртуальных, и облачных. Кроме того, он дает возможность осуществлять контроль за изменениями и использовать уникальное сочетание технологий черных и белых списков, не имеющее себе равных в отрасли.

В комплект McAfee Server Security Suite Advanced включен McAfee Application Control for Servers — решение для создания белых списков, позволяющее запускать на серверах только одобренное программное обеспечение. В этом централизованно управляемом решении, работающем по принципу белого списка, используется динамическая модель доверия и инновационные функции безопасности, которые блокируют несанкционированные приложения и сводят на нет постоянные угрозы повышенной сложности (APT), позволяя при этом отказаться от трудоемкой работы по составлению списков. Технология белых списков лишь незначительно снижает быстродействие узла, поскольку защита от угроз осуществляется без обновления сигнатур.

Базовый функционал защиты серверов обеспечивается, среди прочего, традиционными решениями для защиты от вредоносных программ, предназначенными для серверов под управлением Microsoft Windows и Linux. В их число входит программное обеспечение McAfee VirusScan® Enterprise, занявшее первое место в проведенном компанией NSS Labs тестировании продуктов для защиты от средств использования уязвимостей «нулевого дня» и техник обхода защиты. Помимо традиционных средств защиты от вредоносных программ в комплект входит также отдельное решение, предназначенное для виртуальных сред. Антивирусное решение McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus оптимизировано для виртуализированных сред: оно не оказывает значительного влияния на быстродействие даже очень больших сред и поддерживает гипервизоры всех основных производителей. McAfee MOVE AntiVirus можно приобрести либо в безагентном варианте, настроенном на развертывание в средах VMware, либо в многоплатформенном варианте, который

можно развернуть в средах, созданных на основе гипервизоров KVM, Microsoft Hyper-V, VMware и Xen.

Хотя антивирусные технологии играют ключевую роль в обеспечении защиты, в случае сложных угроз могут потребоваться дополнительные решения. McAfee Host Intrusion Prevention обеспечивает защиту от сложных угроз безопасности, которые в противном случае могут случайно или преднамеренно попасть в организацию.

Кроме того, благодаря интеграции с брандмауэром VMware vCNS App Firewall появился брандмауэр McAfee Agentless Firewall. Он дает администратору возможность управлять одним или несколькими экземплярами VMware vShield App Firewall, используя для этого платформу McAfee ePO, и иметь единый интерфейс для управления политиками брандмауэра во всех виртуальных центрах обработки данных. Кроме того, данное расширение позволяет легко изолировать группы ресурсов без необходимости вручную создавать отдельные сложные правила для брандмауэра. Оно также может обнаруживать любые изменения, внесенные с помощью иных средств, и дает администратору возможность исправить ситуацию одним щелчком мыши.

Расширение инфраструктуры в облако

По мере расширения инфраструктуры в облако становится все труднее следить за применением надлежащих политик безопасности к новым рабочим нагрузкам. McAfee решает эти проблемы путем автоматического обнаружения как запущенных, так и остановленных виртуальных машин, развертываемых в частных и публичных облаках. Для использования этой функции необходимо просто зарегистрировать учетную запись публичного облака в платформе McAfee ePO. Это даст возможность автоматически обеспечить защиту виртуальных машин с помощью соответствующих политик безопасности. Кроме того, панель мониторинга решений McAfee для защиты центров обработки данных дает возможность получать полную информацию об уровне защиты и инцидентах безопасности в частных и публичных облаках.

Оптимизация серверов — это оптимизация 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 компанией McAfee комплект решений позволяет обеспечивать безопасность серверов любого типа — физических, виртуальных и

облачных. Комплект McAfee Server Security Suite Advanced — это набор средств защиты серверов в физических, виртуальных и облачных средах, включающий в себя передовые решения для обеспечения и поддержания надежного уровня безопасности в масштабах всей организации.

Дополнительную информацию о преимуществах McAfee Server Security Suite Advanced можно получить по адресу: www.mcafee.com/ru/products/server-security-suite-advanced.aspx.

Функция	Назначение
Белые списки приложений	<ul style="list-style-type: none"> Значительно меньшее влияние на быстродействие узла по сравнению с традиционными решениями для защиты конечных точек Защита от угроз «нулевого дня» и постоянных угроз повышенной сложности (APT) без обновления сигнатур, значительно сокращающая время, необходимое для обеспечения защиты Динамические белые списки, требующие меньших эксплуатационных издержек по сравнению с прежними методами на основе белых списков
Контроль за изменениями	<ul style="list-style-type: none"> Предотвращение внесения несанкционированных изменений в критически важные системные файлы, каталоги и настройки, позволяющее администраторам экономить время на устранении нарушений безопасности Отслеживание и проверка в режиме реального времени всех попыток внесения изменений на вашем сервере, с соблюдением политики изменений по временному интервалу, источнику или уведомлению о разрешении изменений Постоянный контроль, минимизирующий воздействие незапланированных или несанкционированных изменений
Управление из единой консоли	<ul style="list-style-type: none"> Централизованное управление физическими и виртуальными серверами, включая серверы, расположенные в облаке (как в частном, так и в публичном), позволяющее собирать больше информации о степени защищенности серверов Упрощение оперативных аспектов и сокращение временных затрат административного персонала Снижение затрат на оборудование в связи с сокращением количества необходимых серверов
Базовая защита серверов	<ul style="list-style-type: none"> Средство антивирусной защиты для физических серверов, занявшее первое место в проведенном компанией NSS Labs¹ тестировании продуктов для защиты от средств использования уязвимостей «нулевого дня» и от попыток обхода защиты Host Intrusion Prevention для защиты от сложных угроз безопасности, которые в противном случае могут случайно или преднамеренно попасть в организацию
Безопасность систем виртуализации	<ul style="list-style-type: none"> Оптимизированная защита рабочих нагрузок, развернутых в виртуальных инфраструктурах, без снижения быстродействия и эффективности использования ресурсов Защита разных типов гипервизоров, что позволяет поддерживать общий статус защищенности для всех типов гипервизоров, используемых в центре обработки данных Оптимизированное безагентное развертывание в средах на базе VMware, позволяющее повысить уровень быстродействия и плотность виртуальных машин
McAfee Agentless Firewall	<ul style="list-style-type: none"> Возможность получать информацию обо всех виртуальных сетевых изоляциях посредством отчетов McAfee ePO Возможность контролировать и изолировать виртуальные машины и данные благодаря интеграции с VMware vCNS App Firewall
Полный сбор информации о виртуальных машинах в облаке (как в частном, так и в публичном)	<ul style="list-style-type: none"> Обнаружение не только физических серверов, но и гипервизоров и виртуальных машин в средах VMware vSphere, Amazon AWS, OpenStack и Microsoft Azure, позволяющее получить полную картину активов, подлежащих защите Обнаружение виртуальных машин по мере их инициализации и их автоматическая защита с помощью политик безопасности, позволяющих обеспечить надлежащий уровень защищенности этих виртуальных машин

1. NSS Labs, Inc., Protection & Evasion Test (Результаты тестирования защиты от техник обхода, проведенного компанией NSS Labs), 2013 г.



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

Intel и логотип Intel являются зарегистрированными товарными знаками Intel Corporation в США и/или других странах. McAfee, логотип McAfee, ePolicy Orchestrator, McAfee ePO и VirusScan являются товарными знаками или зарегистрированными товарными знаками корпорации McAfee, Inc. или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Планы выпуска продуктов, спецификации и описания, приведенные в настоящем документе, предоставляются только в информационных целях и могут подвергаться изменениям без предварительного извещения; они поставляются без предоставления гарантии какого-либо вида, явной или подразумеваемой. Copyright © 2015 McAfee, Inc. 61953ds_sss-adv_0515