Краткая деловая информация

Продукты McAfee для защиты серверов

Защита серверных рабочих нагрузок с минимальными потерями быстродействия и эффективным механизмом управления

Представьте, что вы столкнулись с необходимостью выбирать между обеспечением защиты всех серверов в вашем ЦОД — физических и виртуальных — и оптимизацией их быстродействия. Что вы выберете? Если вы выберете защиту, то вам будет легче обеспечить высокий уровень доступности своих ИТ-служб, защитить свои данные и превосходно пройти очередной аудит нормативно-правового соответствия. Если вы выберете быстродействие, то сможете поднять уровень отдачи от своих инвестиций в аппаратное и программное обеспечение, не говоря уже о похвале со стороны финансового директора. Так что же вы выберете: защиту или быстродействие? А теперь представьте, что выбирать не нужно, и что можно получить и то, и другое!

На распутье между защитой и быстродействием

В самом деле, быстрая виртуализация центров обработки данных ставит многих ИТ-директоров именно перед таким выбором. 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 из них 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 серверах необходимо обязательно устанавливать средства обеспечения безопасности, иначе произойдет катастрофа. Но дело в том, что большинство имеющихся технологий обеспечения безопасности были разработаны для защиты выделенных физических систем. Они не успевают за темпами развития технологий виртуализации и не соответствуют требованиям современных смешанных центров обработки данных. В настоящее время существует острая потребность в таких решениях для защиты серверов, которые:

- обеспечивают уникальную и разную защиту всех основных рабочих нагрузок центров обработки данных, включая серверы баз данных, веб-серверы, серверы приложений, почтовые серверы, серверы коллективной работы и серверы хранения данных. В недавно опубликованном компанией SANS Institute документе[1] отмечается, что для обеспечения комплексной защиты серверов необходимо провести развертывание целого ряда технологий, позволяющих безопасно подготавливать серверы к работе, управлять уязвимостями в их временной динамике, защищать доступ к информации, быстро выявлять угрозы по мере их появления и повысить эффективность операций по обеспечению сетевой безопасности;
- не конкурируют с бизнес-службами за мощности процессора. Традиционные решения для обеспечения безопасности обычно потребляют значительное количество свободных вычислительных ресурсов. Это происходит во многом из-за их чрезмерной зависимости

Ключевые преимущества

Оптимизация системы безопасности. Минимизация потерь быстродействия. Использование комплектов McAfee Server Security Suite Essentials и McAfee Server Security Suite Advanced позволяет отказаться от поиска компромиссов между защитой и быстродействием серверов в современных виртуализированных центрах обработки данных.

Каждый из этих комплектов представляет собой сочетание технологий черных списков и поддержки виртуализации, позволяющее обеспечить комплексную защиту ключевых рабочих нагрузок на физических и виртуальных серверах с общей нагрузкой на процессор не выше 5 %. McAfee Server Security Suite Advanced имеет ряд дополнительных защитных функций, таких как белые списки и контроль за изменениями.

Все комплекты поддерживают централизованное управление, осуществляемое с помощью программного обеспечения McAfee ePO.

McAfee предлагает следующие комплекты:

- McAfee Server Security Suite Essentials
- McAfee Server Security Suite Advanced
- McAfee Security Suite for VDI
- McAfee Data Center Security Suite for Databases

intel Security

от технологий черных списков на основе сигнатур, которым для обнаружения угроз приходится постоянно по несколько раз сканировать весь образ системы;

- обеспечивают оптимальную поддержку всех основных сред виртуализации;
- позволяют управлять всеми элементами системы безопасности в масштабах всей серверной среды, включающей в себя как физические, так и виртуальные серверы, с помощью единой консоли управления.

Комплекты McAfee для защиты серверов

Для выполнения этих требований и для обеспечения безопасности современных крайне виртуализированных центров обработки данных McAfee предлагает ряд комплектов для защиты серверов, разработанных с учетом потребностей конкретных рабочих нагрузок на серверах под управлением Microsoft Windows и Linux.

Чтобы обеспечить максимально возможный уровень защиты серверов, в McAfee Server Security Suite Advanced используется сочетание белых списков (позволяющих, например, осуществлять контроль за приложениями) с черными списками на основе сигнатур (позволяющими обеспечивать антивирусную защиту и предотвращать вторжения на узел). Сразу после сканирования систем данный комплект устанавливает блокировку на запуск неавторизованных приложений, тем самым защищая системы от проникновения вредоносных программ. Это приводит к сильному сокращению частоты сканирования систем с использованием сигнатур и сводит к минимуму нагрузку на процессор, что является значительным преимуществом для любой компании. Уникальное сочетание белых списков, черных списков и функций поддержки виртуализации позволяет добиться недостижимой ранее оптимизации операций в ЦОД путем максимизации уровня безопасности как физических, так и виртуальных серверов при минимальных потерях быстродействия. Все компоненты каждого комплекта тесно интегрированы с платформой управления безопасностью McAfee® ePolicy Orchestrator® (McAfee ePO™), что обеспечивает эффективный централизованный подход к оценке рисков, управлению безопасностью и реагированию на инциденты.

McAfee Data Center Security Suite for Databases сочетает в себе функции глобального обнаружения баз данных, комплексной оценки уязвимостей и неинтрузивного мониторинга активности в режиме реального времени по всем направлениям угроз. В комплект входят следующие средства защиты:

- McAfee Database Activity Monitoring
- McAfee Vulnerability Manager for Databases

McAfee Server Security Suite Essentials содержит полный набор функций для обеспечения базовой защиты на серверах всех типов (черные списки, оптимизированная поддержка виртуализации). McAfee Server Security Suite Advanced привносит такие защитные функции, как белые списки и контроль за изменениями.

McAfee Security Suite for VDI обеспечивает комплексную защиту виртуальных рабочих станций, не снижая уровень быстродействия и не мешая работе пользователей. В комплект входят следующие средства защиты:

- McAfee Application Control for Desktops
- McAfee VirusScan® Enterprise
- McAfee VirusScan Enterprise for Linux
- McAfee MOVE AntiVirus for Virtual Desktops (VDI)
- McAfee ePO (ПО)

McAfee предлагает также следующие решения:

- McAfee Security for Microsoft SharePoint
- McAfee Security for Email Servers
- McAfee VirusScan Enterprise for Storage

Решения McAfee для защиты центров обработки данных

	McAfee Server Security Suite Essentials	McAfee Server Security Suite Advanced	McAfee Security Suite for VDI	McAfee Data Center Security Suite for Databases
McAfee VirusScan Enterprise (ПО)	■	■	■	
McAfee VirusScan Enterprise for Linux (для рабочих станций)			■	
McAfee VirusScan Enterprise for Linux (для серверов)	■	■		
McAfee VirusScan Command Line	■	■		
McAfee Application Control for Servers		■		
McAfee Application Control for Desktops			■	
McAfee MOVE AntiVirus for Virtual Desktops (VDI)			■	
McAfee MOVE AntiVirus for Virtual Servers	■	■		
McAfee MOVE Scheduler	■	■		
McAfee Data Center Connector for VMware vSphere	■	■		
McAfee Data Center Connector for Amazon AWS	■	■		
McAfee Data Center Connector for OpenStack	■	■		
McAfee Data Center Connector for Microsoft Azure	■	■		
McAfee Host Intrusion Prevention	■	■		
McAfee Deep Defender for Servers	■	■		
McAfee Change Control		■		
McAfee Agentless Firewall		■		
McAfee ePO (ПО)	■	■	■	
McAfee File and Removable Media Protection			■	
McAfee Database Activity Monitoring				■
McAfee Vulnerability Manager for Databases				■
Формат лицензии	Экземпляр ОС (на каждую виртуальную машину)	Экземпляр ОС (на каждую виртуальную машину)	На каждую виртуальную машину	Экземпляр базы данных

Самый полный из имеющихся в отрасли наборов технологий защиты серверов

Предоставить такой всеобъемлющий набор решений для защиты серверов может только McAfee, потому что только у McAfee есть весь спектр технологий защиты физических и виртуальных серверов в сочетании с технологиями централизованного управления сложными решениями для обеспечения безопасности в смешанных средах. В этих комплектах используются разные компоненты беспрецедентно обширного портфеля защитных технологий McAfee, в том числе:

- **McAfee VirusScan Enterprise** блокирует и удаляет вредоносные программы. Этот программный продукт сочетает возможности защиты от вирусов и шпионских программ с технологиями брандмауэра и предотвращения вторжений. Он также охватывает и новые угрозы безопасности, снижает издержки на реализацию ответных мер в случае эпидемий и оказывает наименьшее в отрасли влияние на работу системы.
- **McAfee VirusScan Enterprise for Linux** обеспечивает превосходную постоянную защиту против все возрастающего количества вирусов, червей и вредоносного кода для систем Linux. Программный пакет McAfee VirusScan Enterprise for Linux, предназначенный для современных динамичных компаний, обеспечивает простоту масштабирования, автоматическую установку обновлений и централизованное управление с помощью единой консоли — платформы McAfee ePO.
- **McAfee Application Control** предлагает эффективный способ блокирования неразрешенных приложений и кода на серверах, корпоративных настольных системах и устройствах с фиксированными функциями. В этой технологии списков доверенных приложений (белых списков) с централизованным управлением используются динамическая модель доверия и новейшие защитные функции, отражающие постоянные угрозы повышенной сложности без необходимости обновления сигнатур и трудоемкого управления списками.
- **McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus** оптимизирует антивирусную защиту McAfee для виртуальных рабочих станций и серверов без снижения уровня производительности и безопасности, помогая вам реализовать операционные выгоды и повысить эффективность управления системой безопасности. McAee MOVE AntiVirus обеспечивает защиту вашего виртуального окружения, включая ваши виртуальные машины в «облаке».
- **Соединительные модули McAfee Data Center Connector** дают возможность собирать полную информацию о состоянии виртуальных машин. Вы сможете обнаруживать не только физические серверы, но и гипервизоры и виртуальные машины в средах VMware vSphere, Amazon Web Services, OpenStack и Microsoft Azure. Собрав информацию о предоставлении виртуальных машин в вашем публичном «облаке», вы сможете определить, какие из них подлежат автоматической защите с помощью соответствующих политик безопасности.
- **McAfee Host Intrusion Prevention for Server** обеспечивает упреждающую защиту от известных и новых атак «нулевого дня». Его использование повышает уровень безопасности и сокращает расходы за счет снижения частоты и степени срочности установки исправлений. Интеграция McAfee Host Intrusion Prevention с платформой McAfee ePO предоставляет в ваше распоряжение централизованные средства отчетности и управления, отличающиеся высокой точностью, масштабируемостью, простотой в использовании и совместимостью с другими продуктами McAfee и сторонних компаний.
- **McAfee Deep Defender for Servers** — это следующее поколение средств защиты конечных точек с аппаратной поддержкой, использующее технологию McAfee DeepSAFE™, работающее за пределами операционной системы и позволяющее обнаруживать, блокировать и предотвращать сложные скрытые атаки. McAfee Deep Defender представляет собой новый подход к обеспечению безопасности. Это первый продукт, созданный на основе технологии McAfee DeepSAFE, разработанной совместно с Intel.
- **McAfee Change Control** позволяет избежать внесения таких изменений в серверных средах, которые могут привести к нарушению системы безопасности, утечке данных или сбою в работе. McAfee Change Control облегчает обеспечение соответствия нормативно-правовым актам.

- **McAfee Agentless Firewall** дает возможность получать информацию обо всех уровнях изоляции виртуальных сетей. Благодаря интеграции с VMware vCNS App Firewall это решение позволяет управлять виртуальными машинами и данными, а также изолировать их.
- **McAfee File and Removable Media Protection** обеспечивает защиту данных, находящихся на внутренних и съемных носителях, при помощи шифрования. Решение дает возможность шифровать съемные USB-накопители и безопасно передавать информацию.
- **McAfee Database Activity Monitoring** автоматически обнаруживает имеющиеся в вашей сети базы данных, обеспечивает их безопасность с помощью ряда готовых к использованию средств защиты и помогает вам создать индивидуальную политику безопасности для вашего окружения. Решение экономически эффективно обеспечивает защиту ваших данных от всех угроз путем локального мониторинга действий на каждом сервере баз данных и путем рассылки оповещений или пресечения вредоносных действий в режиме реального времени даже при работе в виртуальной или облачной среде.
- **McAfee Vulnerability Manager for Databases** позволяет получить оперативную, точную и полную картину уязвимостей на всех ваших активах, соединенных в сеть. Он помогает опережать эволюционирующие угрозы, а также назначать приоритеты мерам противодействия благодаря наличию единого коррелированного представления уязвимостей, имеющихся в вашей среде.
- **Программное обеспечение McAfee ePO** обеспечивает централизованное управление физическими и виртуальными серверами, в том числе расположенными в частных и общедоступных «облаках». Управляя всеми конечными точками из единой консоли, вы 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.

Успех комплектов для защиты серверов

Комплекты McAfee для защиты серверов 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. Для получения подробной информации посетите веб-сайт компании McAfee по адресу **www.mcafee.com/ru/products/data-center-security/index.aspx**.

1. **www.sans.org/reading_room/analysts_program**

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