McAfee Public Cloud Server Security Suite

Комплексная защита серверов для пользователей публичного облака

Ключевые преимущества
McAfee Public Cloud Server Security Suite дает вам следующие возможности:

- Сбор информации о появляющихся и исчезающих экземплярах облачных серверов. Обнаружение экземпляров серверов в публичном облаке с помощью соединительных модулей McAfee Data Center Connector, помогающих обеспечить единообразную конфигурацию и применение политик даже в тех организациях, в которых существует проблема «теневых информационных технологий».
- Защита экземпляров серверов с помощью уникального сочетания средств антивирусной защиты, установленных на узле брандмауэров, белых списков приложений, средств защиты от вторжений и технологий защиты данных во всех реализациях публичных облаков, работающих в средах под управлением Microsoft Windows или Linux.
- Управление политиками обеспечения безопасности экземпляров серверов в публичном облаке в соответствии с уже имеющимся наработками с помощью единой платформы управления.

Переходя на использование экземпляров облачных серверов, размещенных в публичном облаке, в качестве дополнительных, а нередко даже основных компонентов своих центров обработки данных, предприятия отдают себе отчет в том, что одним из ключевых факторов успеха такой стратегии является использование модели совместного обеспечения безопасности. Поставщики публичных облачных сред, такие как Amazon Web Services (AWS) и Microsoft Azure, обеспечивают защиту периметра, а защиту содержимого должны обеспечивать пользователи. Поэтому перед дальновидными предприятиями встает вопрос о том, как обеспечить защиту от угроз «нулевого дня» и сложных постоянных угроз, сохраняя при этом расходы на уровне, соответствующем их стратегии использования облачных технологий.

Комплект McAfee® Public Cloud Server Security Suite обеспечивает комплексную защиту серверов в публичном облаке, помогая перенести политики обеспечения безопасности физических серверов на серверы в публичном облаке и управлять ими. McAfee Public Cloud Server Security Suite дает возможность собирать информацию о том, что происходит с экземплярами серверов в публичном облаке, обеспечивать комплексную защиту, используя эффективное сочетание черных и белых списков, а также динамически управлять этой средой, настольными системами, мобильными устройствами и локальными серверами с помощью программного обеспечения McAfee® ePolicy Orchestrator® (McAfee ePO™).

Оптимизация для работы с публичным облаком

ИТ-специалистам, уделяющим должное внимание безопасности, необходима возможность так управлять рисками, чтобы уровень безопасности данных в облаке не отличался от того уровня, который они считают обязательным при использовании локальных серверов. В комплекте McAfee Public Cloud Server Security Suite, оптимизированном для облачных пользователей, используются те же самые технологии мирового класса (McAfee VirusScan® Enterprise и система предотвращения вторжений [IPS]), которые применяются и в наших комплектах McAfee Server Security Suite Essentials и McAfee Server Security Suite Advanced.

Одним из основных средств защиты серверов в комплекте McAfee Public Cloud Server Security Suite является решение

Поддерживаемые платформы

- Windows Server 2008, 2008 R2, 2012, 2012 R2
- Linux (Red Hat, CentOS, SUSE, Ubuntu, Amazon Linux)

VirusScan Enterprise, предназначенное для защиты экземпляров серверов под управлением Microsoft Windows или Linux от вредоносных программ. Хотя антивирусные технологии играют ключевую роль в обеспечении защиты, в случае сложных угроз могут потребоваться дополнительные решения. McAfee Host Intrusion Prevention for Server обеспечивает защиту от сложных угроз безопасности, которые в противном случае могут случайно или преднамеренно попасть в организацию.

В комплект McAfee Public Cloud Server Security Suite 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.

Блокируя несанкционированный сетевой трафик, брандмауэр для систем под управлением Linux и Windows предотвращает проникновение вредоносных программ и бот-сетей на облачные серверы, пресекая тем самым их распространение. Пользователи могут быть уверены в том, что их тома Amazon EBS будут защищены и зашифрованы. Кроме того, в их распоряжении удобная функция шифрования томов, на которых уже есть данные.

Интеллектуальная защита публичного облака

Для защиты облачных серверов необходима дополнительная система безопасности, для управления которой у клиентов нет достаточных ресурсов. И когда для работы над краткосрочными внутренними проектами сотрудники начинают использовать публичные облака, не соблюдая надлежащий протокол ИТ-безопасности, ранее непроницаемые защитные стены могут быстро стать ненадежными, а риск нарушения безопасности может вырасти экспоненциально. McAfee Public Cloud Server Security Suite подразумевает использование широкого набора функций программного обеспечения McAfee ePO, позволяющего выявлять угрозы, управлять средствами защиты и генерировать отчеты в масштабах всей серверной инфраструктуры, состоящей из физических, виртуальных и облачных систем. Программное обеспечение McAfee ePO обеспечивает централизованный сбор информации о происходящем с этими «теневыми информационными технологиями» и является в высшей степени масштабируемой, гибкой и автоматизированной платформой для централизованного управления и применения политик управления средствами защиты, позволяющей выявлять проблемы и угрозы безопасности и реагировать на них.

Кроме того, по мере всё большего распространения средств DevOps критически важное значение приобретает необходимость обеспечения беспрепятственного взаимодействия с такими средствами. McAfee Public Cloud Server Security Suite беспрепятственно взаимодействует с такими новейшими средствами DevOps, как Chef и Puppet Labs.

Экономичность и гибкость

При расширении бизнеса важную роль играет способность ИТ-подразделения быстрее реагировать на меняющиеся инфраструктурные потребности. В настоящее время для удовлетворения этих потребностей многие ИТ-подразделения используют решения в категории «Инфраструктура как услуга» (Infrastructure-as-a-Service — IaaS), помогающие сократить расходы и сделать инфраструктуру более динамичной и масштабируемой. Кроме того, переход на использование IaaS с целью удовлетворения растущих инфраструктурных потребностей приводит к тому, что многие компании меняют структуру своих расходов, снижая

долю капитальных и увеличивая долю операционных затрат. Динамический характер таких сред требует, чтобы цены на защитные программные решения были соразмерны ценам используемой вычислительной инфраструктуры. McAfee Public Cloud Server Security Suite оплачивается на почасовой основе: это дает клиентам возможность платить за защиту серверов в оптимальном соответствии со своими финансовыми целями и при этом вписывается в модель потребления вычислительных ресурсов в рамках инфраструктуры IaaS.

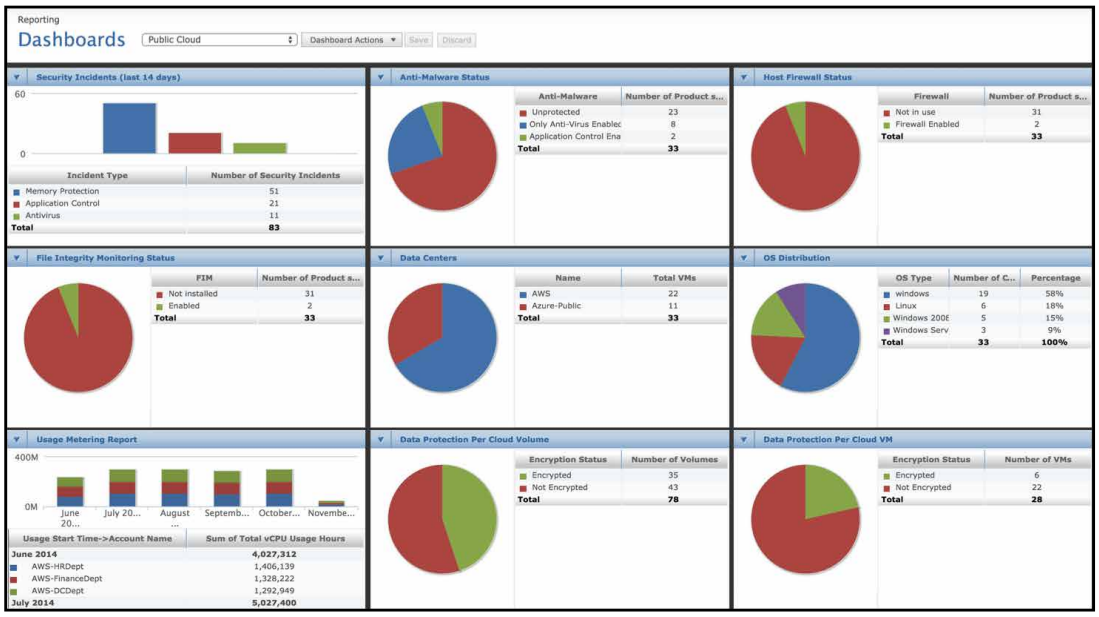

Рис. 1. Единая панель мониторинга для McAfee Public Cloud Server Security Suite

Функция	Преимущество	Преимущества для клиентов
Централизованное управление с помощью программного обеспечения McAfee ePO	Наличие единой консоли позволяет обеспечить комплексное управление всеми функциональными возможностями McAfee по защите конечных точек	• 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
Модули McAfee Data Center Connector для Amazon Web Services (AWS), Microsoft Azure и OpenStack	Полная видимость виртуальных серверов, находящихся в публичных облачных инфраструктурах	• Возможность обнаруживать экземпляры серверов в публичных облачных средах Amazon AWS, Microsoft Azure и OpenStack, позволяющая получать полную картину активов, подлежащих защите • Полная видимость всех инициализированных экземпляров, позволяющая автоматически обеспечивать надежную защиту этих экземпляров с помощью политик безопасности
Защита данных в облаке	Управление шифрованием томов Amazon EBS, доступных в зарегистрированных учетных записях Amazon AWS	• Шифрование, помогающее обеспечивать защиту данных и интеллектуальной собственности от несанкционированного доступа • Возможность зашифровывать тома, на которых уже есть данные, непосредственно из программного обеспечения McAfee ePO • Минимальное снижение уровня быстродействия благодаря использованию встроенных функций шифрования Amazon EBS

Функция	Преимущество	Преимущества для клиентов
VirusScan Enterprise для серверов	Основные функции защиты от вредоносных программ для серверов Windows и Linux	• Оптимизация для обеспечения высокого уровня быстродействия и сокращения объема потребляемых системных ресурсов, что помогает добиться оптимальной производительности серверов • Максимальная защита от вредоносных программ: защита систем и файлов от вирусов, шпионских программ, червей, троянов и других рисков; обнаружение и удаление вредоносных программ; возможность для пользователей легко настраивать политики для управления объектами, находящимися в карантине • Упреждающая защита от атак: сканирование в режиме реального времени, обеспечивающее защиту всех систем, включая удаленные объекты, от известных и новых угроз. VirusScan Enterprise также обеспечивает защиту от средств использования уязвимостей приложений Microsoft, вызывающих переполнение буфера
Предотвращение вторжений на узел (IPS)	Система IPS обеспечивает критически важную и необходимую защиту от известных угроз и угроз «нулевого дня»	• Решение McAfee Host Intrusion Prevention, обеспечивающее защиту от сложных угроз безопасности, которые в противном случае могут случайно или неслучайно попасть внутрь компании • Технология следующего поколения, обеспечивающая более надежную защиту от вирусов, червей, троянских коней и других угроз, способных украсть ваши критически важные данные или вызвать простой в работе вашей компании. Она защищает от атак ваши самые уязвимые приложения, тем самым избавляя вас от тревог • Защита ваших устройств от вирусов, проникающих внутрь компании через съемные носители, веб-трафик и удаленную сеть
Брандмауэр для Linux и Windows	Резидентный брандмауэр для защиты экземпляра сервера от несанкционированного доступа и атак	• Предотвращение проникновения вредоносного ПО на экземпляр сервера и распространения в публичном облаке
Контроль за приложениями	Обеспечивает постоянное соответствие узлов заведомо «безопасному» эталону благодаря предотвращению запуска нежелательных приложений	• Значительное снижение влияния 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	Позволяет осуществлять мониторинг целостности файлов путем непрерывного отслеживания изменений, вносимых на системном уровне во всех точках распределенной сети, включая удаленные объекты	• 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

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

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