McAfee Cloud Workload Security

Защитите свои рабочие нагрузки в частных и публичных облаках! Безопаснее. Быстрее. Проще.

В результате развития корпоративных центров обработки данных растет количество рабочих нагрузок, ежедневно переносимых в облачные среды. В большинстве организаций используется гибридная среда, состоящая как из локальных, так и из облачных рабочих нагрузок (включая контейнеры), находящихся в процессе постоянного изменения. Такая практика осложняет задачу обеспечения безопасности, поскольку облачные среды (частные и публичные) требуют новых подходов и новых средств защиты. Организациям требуются централизованный сбор информации обо всех облачных рабочих нагрузках, а также их комплексная защита от риска ошибок в конфигурации, заражения вредоносными программами и утечек данных.

Решение McAfee® Cloud Workload Security автоматизирует процессы обнаружения и защиты эластичных рабочих нагрузок и контейнеров, что позволяет избавиться от «мертвых зон», обеспечить защиту от сложных угроз и упростить процедуру управления многооблачными средами. С помощью единой автоматизированной политики McAfee обеспечивает беспрецедентно высокий уровень защиты ваших рабочих нагрузок при их переходе из одной виртуальной (частной, публичной или гибридной) среды в другую, что позволяет вашим сотрудникам отделов ИБ существенно повысить эффективность работы.

Сбор информации в режиме реального времени

Автоматическое обнаружение

Невидимые экземпляры рабочих нагрузок и контейнеры Docker создают бреши в управлении безопасностью и могут стать тем плацдармом, который необходим злоумышленникам для проникновения в вашу организацию. McAfee Cloud Workload Security обнаруживает экземпляры эластичных рабочих нагрузок и контейнеры Docker в средах на базе Amazon Web Services (AWS), Microsoft Azure и VMware и непрерывно

Ключевые преимущества

- Непрерывный сбор информации об экземплярах эластичных рабочих нагрузок позволяет устранить «мертвые зоны» рабочей среды и одновременно автоматизировать ранее трудоемкий процесс внедрения политик.
- Помимо обнаружения и мониторинга контейнеров Docker вы сможете обеспечивать их безопасность с помощью технологии микросегментации.
- Оптимизированная под виртуальные машины защита от угроз обеспечивает многоуровневые меры противодействия.
- Централизованное управление и автоматизированные рабочие процессы значительно уменьшают сложность гибридных и многооблачных сред.

Подписаться

отслеживает новые экземпляры. Вы получаете централизованное и полное представление о разных средах и устраняете «мертвые зоны» (с точки зрения работы и безопасности), которые подвергают вас риску.

Современные средства защиты рабочих нагрузок

Защита от сложных угроз

Для защиты ваших рабочих нагрузок от программ-вымогателей, целенаправленных атак и других угроз McAfee Cloud Workload Security сочетает в себе комплексные меры противодействия: технологии машинного обучения, средства сдерживания приложений, средства защиты от вредоносных программ, оптимизированные под виртуальные машины, белые списки, механизмы мониторинга целостности файлов и технологию микросегментации. Решение Advanced Threat Protection, оснащенное технологией машинного обучения, позволяющей выявлять вредоносное содержимое на основе анализа поведения и атрибутов кода, использует эту технологию для отражения изощренных, ранее не встречавшихся атак.

Консолидация событий

McAfee Cloud Workload Security позволяет организациям управлять большим количеством защитных технологий как в локальных, так и в облачных средах с помощью единого интерфейса управления. Сюда относятся и такие технологии сторонних производителей, как AWS GuardDuty. Администраторы могут использовать имеющиеся в AWS GuardDuty средства непрерывного мониторинга и обнаружения несанкционированного поведения, получая тем самым еще один уровень сбора информации об угрозах. Эта интеграция дает пользователям McAfee Cloud Workload Security возможность просматривать события GuardDuty, к которым относятся сетевые подключения, зондирование портов и DNS-запросы по экземплярам EC2, непосредственно в консоли McAfee Cloud Workload Security. Когда трафик соответствуют трафику, обнаруженному с помощью McAfee Cloud Workload Security, производится сопоставление событий GuardDuty, относящихся к сетевым подключениям, в потоковом графе.

Превосходная защита виртуальных сред

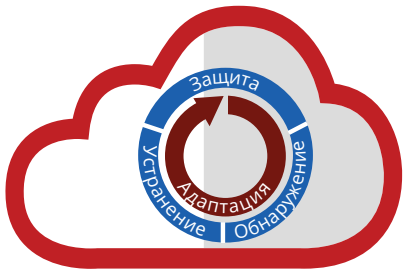
McAfee Cloud Workload Security защищает ваши виртуальные машины в частном облаке от вредоносного ПО, не создавая дополнительной нагрузки на базовые ресурсы и не увеличивая эксплуатационные расходы. Вы получаете защиту от вредоносных программ, которая осуществляет интеллектуальное планирование ресурсоемких задач (например, сканирования по запросу), которые выполняются в то время, когда гипервизор не перегружен.

Визуализация сети с использованием микросегментации

Использование встроенных в облако средств визуализации сети, механизма рассылки приоритизированных оповещений о рисках и технологии микросегментации обеспечивает такой уровень осведомленности и контроля,

Ключевые преимущества (продолжение)

- Интеграция с такими инструментами автоматизации, как Chef и Puppet, позволяет применять меры обеспечения безопасности к рабочим нагрузкам в публичных и частных облаках во время развертывания.
- Простая в использовании многоуровневая защита от сложных вредоносных программ и вторжений.
- Визуализация и обнаружение сетевых угроз — без установки агента.
- Защита среды, исправляя ситуацию исправлению ситуации непосредственно в рамках предлагаемого решения.



Cloud Workload Security

Комплексный **сбор информации** и **контроль**

который необходим для предотвращения развития межузловых атак в виртуальных средах и атак из внешних неблагонадежных источников. Функция завершения работы или помещения в карантин одним щелчком мыши помогает снизить риск ошибок конфигурации и повышает эффективность мер по устранению уязвимостей.

Мониторинг целостности файлов

Механизмы мониторинга целостности файлов постоянно следят за тем, чтобы ваши системные файлы и каталоги не были взломаны вредоносными программами, хакерами или злоумышленниками внутри самой компании. Данные комплексного аудита содержат информацию о том, как изменяются файлы на серверных рабочих нагрузках, и предупреждают вас о наличии активной атаки.

Контроль за приложениями

Использование белых списков приложений предотвращает как известные, так и неизвестные атаки, обеспечивая работу только доверенных приложений и блокируя любые несанкционированные вредоносные нагрузки. Функция контроля за приложениями обеспечивает динамическую защиту на основе информации о локальных и глобальных угрозах, а также возможность своевременного обновления систем без отключения функций безопасности.

Упрощенное управление

Унификация путем централизованного управления

Единая консоль обеспечивает единообразную политику безопасности и централизованное управление в многооблачных средах на серверах, виртуальных серверах и облачных рабочих нагрузках.

Автоматизированное развертывание

С помощью инструментов автоматизации развертывания, поддержку которых предоставляют такие компании, как Chef, Puppet и Ansible, вы можете автоматически развертывать технические решения по обеспечению безопасности в многооблачных средах.

Повышение уровня безопасности

McAfee Cloud Workload Security позволяет поддерживать безопасность на высочайшем уровне, используя при этом все преимущества облака. Решение объединяет в себе разнообразные технологии защиты, упрощает управление средствами безопасности и защищает предприятие от киберугроз, что дает вам возможность полностью сосредоточиться на развитии бизнеса. Ниже приведено сравнение функций доступных вариантов пакета.

Функции	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
Централизованное управление (платформа McAfee® ePO™)	✓	✓	✓
Поддержка многооблачных сред (AWS, Azure, VMware)	✓	✓	✓
Карантин для рабочих нагрузок и контейнеров с помощью технологии микросегментации	✓	✓	✓
Предотвращение угроз безопасности серверных ОС (Windows и Linux)	✓	✓	✓
Предотвращение локальных вторжений и противодействие средствам эксплуатации уязвимостей	✓	✓	✓
Управление шифрованием в облаке	✓	✓	✓
Встроенные средства управления брандмауэром для AWS и Azure (группы безопасности)	✓	✓	✓
McAfee® Management for Optimized Virtual Environments (безагентный и многоплатформенный)	✓	✓	✓
Локальный брандмауэр	✓	✓	✓
Адаптивная защита от угроз с технологией машинного обучения		✓	✓
Визуализация сетевого трафика с технологией микросегментации		✓	✓
Встроенные облачные средства анализа сетевого трафика в сочетании с оценкой репутации на основе данных сервиса Global Threat Intelligence		✓	✓
Application Control for Servers			✓
File Integrity Monitoring			✓
Change Control for Servers			✓
Интеграция с McAfee® Virtual Network Security Platform		✓	✓

Дополнительная информация

За подробной информацией обращайтесь на сайт **www.mcafee.com/ru/products/cloud-workload-security.aspx**.

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