# McAfee Cloud Workload Security

## Защита рабочих нагрузок в гибридной инфраструктуре. 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 (McAfee® CWS) 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 защиту ваших рабочих нагрузок при их переходе из одной виртуальной (частной, публичной или многооблачной) среды в другую, что позволяет вашим сотрудникам отделов ИБ существенно повысить эффективность работы.

## Современные средства защиты рабочих нагрузок. Примеры использования

### Автоматическое обнаружение

Неуправляемые 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 CWS обнаруживает экземпляры эластичных рабочих нагрузок и контейнеры Docker в средах на базе Amazon Web Services (AWS), Microsoft Azure, OpenStack и VMware.

## Ключевые преимущества

- Непрерывный сбор информации об экземплярах эластичных рабочих нагрузок позволяет устранить «мертвые зоны» рабочей среды и одновременно автоматизировать ранее трудоемкий процесс внедрения политик.
- Централизованное управление и автоматизированные рабочие нагрузки значительно уменьшают сложность гибридных и многооблачных сред.
- Визуализация и обнаружение сетевых угроз — без установки агента.
- Оптимизированная под виртуальные машины защита от угроз обеспечивает многоуровневые меры противодействия.

Подписаться

Кроме того, решение ведет непрерывный мониторинг для обнаружения новых экземпляров. Вы получаете централизованное и полное представление о разных средах и устраняете «мертвые зоны» (с точки зрения работы и безопасности), которые могут вести к возникновению риска.

## Анализ сетевого трафика

Используя платформозависимый сетевой трафик из облачных рабочих нагрузок, McAfee CWS может дополнять и применять информацию об угрозах, поступающую по каналам McAfee® Global Threat Intelligence (McAfee® GTI). Дополненная информация позволяет видеть такие характеристики, как показатель риска, географическое местоположение и другие важные сведения о сети. Эту информацию можно использовать для автоматизированного принятия мер по внесению исправлений, направленных на защиту рабочих нагрузок.

## Интеграция в механизмы развертывания

McAfee CWS создает сценарии развертывания, позволяющие автоматизировать развертывание агента McAfee® (и управление им) в облачных рабочих нагрузках. Эти сценарии позволяют обеспечить интеграцию с инструментами Chef, Puppet и другими средствами DevOps, используемыми для развертывание агента McAfee на рабочих нагрузках, размещенных на серверах AWS, Microsoft Azure или других поставщиков облачных сред.

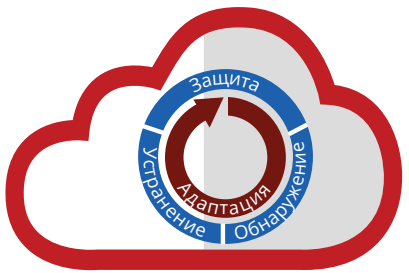
## Консолидация событий

McAfee CWS позволяет организациям управлять большим количеством защитных технологий как в локальных, так и в облачных средах с помощью единого интерфейса управления. Поддерживается также интеграция с другими, дополнительными технологиями: AWS GuardDuty, McAfee® Policy Auditor, McAfee® Network Security Platform и др.

- Администраторы могут использовать имеющиеся в AWS GuardDuty средства непрерывного мониторинга и обнаружения несанкционированного поведения, что дает им еще один уровень сбора информации об угрозах. Пользователи McAfee CWS имеют возможность просматривать события GuardDuty (сетевые подключения, зондирование портов, DNS-запросы по экземплярам EC2 и др.) непосредственно в консоли McAfee CWS.
- McAfee Policy Auditor с помощью агентов проверяет рабочие нагрузки на соответствие известным или заданным пользователем аудитам конфигурации, таким как Закон «О преемственности и подотчетности медицинского страхования» (Health Insurance Portability and Accountability Act — HIPAA), Стандарт безопасности данных в индустрии платежных карт (Payment Card Industry Data Security Standard — PCI-DSS), Эталон Центра интернет-безопасности (Center for Internet Security Benchmark — CIS Benchmark), или другим отраслевым стандартам. Сообщая обо всех выявленных несоответствиях, McAfee CWS обеспечивает мгновенный сбор информации об ошибках в конфигурации облачных рабочих нагрузок.

## 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.
- Вы получите простую систему многоуровневой защиты от сложного вредоносного ПО и вторжений.
- Помимо обнаружения и мониторинга контейнеров Docker вы сможете обеспечивать их безопасность с помощью технологии микросегментации.
- Меры по внесению исправлений и защите среды принимаются непосредственно внутри решения.




Cloud Workload Security

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

- McAfee Network Security Platform — еще одна платформа безопасности облачных вычислений, выполняющая проверку сети на трафик в гибридных средах, а также в средах на базе AWS и Microsoft Azure. Она выполняет более глубокую проверку сетевого трафика на уровне пакетов и сообщает обо всех несоответствиях и предупреждениях через McAfee CWS. Так, в единой унифицированной консоли обеспечивается сбор информации о происходящем в многооблачных средах, что необходимо для устранения уязвимостей.

### Принудительное применение групповых политик сетевой безопасности

McAfee CWS позволяет пользователям и администраторам создавать базовые групповые политики безопасности и проводить аудит политик, применяемых к рабочим нагрузкам, на соответствие этим базовым политикам. При обнаружении любых отклонений от базовых политик или их изменений в консоли McAfee CWS может генерироваться предупреждение. Кроме того, из McAfee CWS администраторы могут вручную настраивать платформозависимые группы сетевой безопасности, что дает им возможность напрямую управлять встроенными в облако групповыми политиками сетевой безопасности.

## Что выделяет McAfee Cloud Workload Security на фоне других решений: основные характеристики и технологии

### Поддержка сборки в облаке

Использование McAfee CWS позволяет нашим клиентам консолидировать управление большим количеством публичных и частных облаков (AWS EC2, виртуальные машины Microsoft Azure, OpenStack, VMware Vcenter и др.) в одной-единственной консоли управления. Новая функция поддержки сборки в облаке для Amazon Elastic Container Service for Kubernetes (Amazon EKS) и Microsoft Azure Kubernetes Service (AKS) дает возможность импортировать приложения и разрешать клиентам запускать их в облаке.

### Упрощенное централизованное управление

Единая консоль обеспечивает единообразную политику безопасности и централизованное управление в многооблачных средах на серверах, виртуальных серверах и облачных рабочих нагрузках. Кроме того, администраторы могут создавать в программном обеспечении McAfee® ePolicy Orchestrator® (McAfee ePO™) большое количество разных разрешений для отдельных ролей, что позволяет внести в определения ролей больше конкретики и точности.

### Визуализация сети с использованием микросегментации

Использование встроенных в облако средств визуализации сети, механизма рассылки приоритизированных оповещений о рисках и технологии микросегментации обеспечивает уровень осведомленности и контроля, позволяющий предотвращать развитие как межузловых атак внутри виртуальных сред, так 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.

### Превосходная защита виртуальных сред

Для защиты используемых в частных облаках виртуальных машин от вредоносного ПО в решении McAfee CWS включен McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus). Примечательно, что защита обеспечивается без создания дополнительной нагрузки на базовые ресурсы и без увеличения эксплуатационных расходов. McAfee MOVE AntiVirus дает организациям возможность оптимизировать защиту виртуализованных сред путем передачи задач обеспечения безопасности на специально выделенные под это виртуальные машины.

Защита пользователей от вредоносных программ осуществляется посредством McAfee® Endpoint Security for Servers. Чтобы не нарушать ход выполнения критически важных бизнес-процессов, решение осуществляет интеллектуальное планирование ресурсоемких задач (например, сканирования по требованию).

### Использование тегов и автоматизация защиты рабочих нагрузок

Возможность импортировать информацию из тегов AWS и Microsoft Azure в программное обеспечение McAfee ePO и назначать политики, исходя из этих тегов, позволяет обеспечить автоматический выбор правильных политик для всех рабочих нагрузок. Управление тегами осуществляется автоматически путем синхронизации имеющихся тегов AWS и Microsoft Azure с тегами в программном обеспечении McAfee ePO.

### Автоматическое внесение исправлений

Политики программного обеспечения McAfee ePO определяются пользователем. Если McAfee CWS обнаружит систему, не защищенную политиками безопасности программного обеспечения McAfee ePO и содержащую вредоносное ПО или вирус, то эта система будет автоматически помещена в карантин.

### Адаптивная защита от угроз

Для защиты ваших рабочих нагрузок от программ-вымогателей, целенаправленных атак и других угроз McAfee CWS 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. McAfee® Advanced Threat Protection отражает изощренные, ранее не встречавшиеся атаки с помощью методов машинного обучения, которые выявляют вредоносное содержимое на основе его поведения и атрибутов кода.

### Контроль за приложениями

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

### Мониторинг целостности файлов

Модуль мониторинга целостности файлов McAfee® постоянно следит 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 в серверных рабочих нагрузках, и предупреждают вас о наличии активной атаки.

## Адекватная защита многооблачных сред

McAfee CWS 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 | McAfee Cloud Workload Security Basic | McAfee® Cloud Workload Security Essentials | McAfee® Cloud Workload Security Advanced |
|---|---|---|---|
| Централизованное управление (платформа McAfee ePO) | ✓ | ✓ | ✓ |
| Поддержка многооблачных сред (AWS, Microsoft Azure, VMware) | ✓ | ✓ | ✓ |
| Карантин для рабочих нагрузок и контейнеров с помощью технологии микросегментации | ✓ | ✓ | ✓ |
| McAfee MOVE (безагентный и многоплатформенный) | ✓ | ✓ | ✓ |
| Модуль для предотвращения угроз McAfee Endpoint Security для серверных ОС (Windows и Linux) | ✓ | ✓ | ✓ |
| Локальный брандмауэр | ✓ | ✓ | ✓ |
| Встроенные средства управления брандмауэром для AWS и Microsoft Azure (группы безопасности) | ✓ | ✓ | ✓ |
| Предотвращение локальных вторжений и противодействие средствам эксплуатации уязвимостей | ✓ | ✓ | ✓ |
| Импорт информации из тегов AWS и Microsoft Azure в программное обеспечение McAfee ePO | ✓ | ✓ | ✓ |
| Автоматическое внесение исправлений в рабочие нагрузки, не соответствующие политикам | ✓ | ✓ | ✓ |
| Адаптивная защита от угроз с технологией машинного обучения | | ✓ | ✓ |
| Визуализация сетевого трафика и микросегментация | | ✓ | ✓ |
| Анализ платформозависимого сетевого трафика в сочетании с оценкой репутации с помощью McAfee GTI | | ✓ | ✓ |
| Интеграция с McAfee® Virtual Network Security Platform (McAfee® vNSP) | | ✓ | ✓ |
| Составление динамических белых списков серверов посредством McAfee Application Control | | | ✓ |
| Непрерывное ведение журналов аудита при помощи модуля мониторинга целостности файлов McAfee | | | ✓ |
| Защита файлов и папок с помощью McAfee® Change Control for Servers | | | ✓ |

## Дополнительная информация

Для получения дополнительной информации посетите страницу **www.mcafee.com/ru/products/cloud-workload-security.aspx**.

Функции и преимущества технологий McAfee зависят от конфигурации системы и могут потребовать активации аппаратного обеспечения, программного обеспечения или услуги. Для получения дополнительной информации посетите веб-страницу www.mcafee.com/ru. Ни одна компьютерная система не может быть полностью защищенной.

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