

# McAfee Web Protection

## Веб-защита в любом варианте: облачное решение, локальное решение, сочетание этих двух вариантов

От фильтрации веб-содержимого и сканирования на наличие вредоносных программ до глубоких проверок содержимого и детального контроля за использованием облачных приложений — решение McAfee® Web Protection обеспечивает необходимые для безопасности предприятия средства защиты и контроля, а также гибкие варианты развертывания. Вам нужны средства контроля на месте, которые дают локально развертываемые решения? Требуется неограниченные возможности масштабирования и низкая стоимость, свойственные облачным услугам? Вы ищете гибридные варианты, сочетающие оба решения? McAfee Web Protection дает вам возможность развернуть веб-защиту таким образом, который будет максимально соответствовать текущим и меняющимся потребностям вашей компании.

Одновременно с расширением и развитием веб-технологий растет число интернет-атак с использованием вредоносных программ, которые угрожают безопасности конечных точек и критически важных данных. Учитывая постоянно возрастающий уровень риска организациям требуется максимально надежная веб-защита, чтобы успешно отражать растущие угрозы. McAfee понимает проблемы безопасности, связанные с использованием современных сетевых и облачных технологий, и предлагает комплексные средства веб-защиты предприятиям, которые заботятся о защите своих активов от угроз.

### Локальное решение, облачное решение или гибридный вариант

Для достижения максимальной гибкости развертывания и долговременной эффективности ваших инвестиций McAfee предлагает все функции продуктов **McAfee Web Gateway** и **McAfee Web Gateway Cloud Service** в едином решении: **McAfee Web Protection**. Решение имеет несколько вариантов развертывания: локальное развертывание с использованием масштабируемого семейства специализированных аппаратных или виртуальных устройств; развертывание в виде облачной службы; и смешанный вариант развертывания, обеспечивающий гибкость

### Ключевые преимущества

#### Максимальная свобода выбора

- Все функции программного обеспечения устройства McAfee Web Gateway и службы McAfee Web Gateway Cloud Service в единой подписке.
- Соответствие требованиям — сегодня. Свобода в выборе схемы внедрения решений — завтра.
- Предсказуемые цены на подписку, зависящие от количества пользователей, а не от варианта развертывания.

#### Передовая защита

- Для блокирования вредоносных программ «нулевого дня» в режиме реального времени в McAfee Web Protection используется модуль McAfee Gateway Anti-Malware Engine, в основе которого лежит запатентованный метод анализа поведения.

## ЛИСТ ДАННЫХ

и доступность корпоративного класса. Например, для защиты сотрудников в корпоративных штаб-квартирах организации могут использовать аппаратные или виртуальные устройства, а для защиты сотрудников, работающих удаленно или в дороге, — облачные службы. Филиалы тоже могут направлять весь свой трафик в облачную службу: это позволит сократить расходы на содержание сетей многопротокольной коммутации пакетов (MPLS), используемых, как правило, для передачи всего публичного веб-трафика на центральный узел с целью его последующей обработки. Какой бы вариант развертывания вы ни выбрали, вы получите передовую систему защиты от вредоносных программ и комплексное решение веб-фильтрации от компании McAfee. Синхронизация управления политиками между локально развернутыми и облачными решениями позволяет обеспечить согласованное применение политик на основе правил на всех платформах.

### Облачная инфраструктура

Технология «инфраструктура как услуга» (IaaS), как например, Amazon Web Services (AWS), обеспечивает динамическую масштабируемость корпоративного уровня и доступ к почти безграничным ресурсам. Специалистам по безопасности необходимо, чтобы их средства веб-защиты и работали в этой среде, и обеспечивали защиту облачных рабочих нагрузок. Для защиты конечных точек, данных и приложений в распоряжении клиентов, использующих McAfee Web Gateway, имеется

несколько вариантов его развертывания: внутри AWS в качестве прокси-сервера переадресации, обратного прокси-сервера или даже сервера ICAP (Internet Content Adaptation Protocol). Это дает организациям возможность направлять более опасный трафик в более продвинутые антивирусные модули. Кроме того, клиенты получают возможность проверять потоки данных на наличие потенциально конфиденциальной информации: для этого они могут использовать либо имеющуюся в McAfee Web Gateway функцию защиты от утечек данных, либо уже имеющееся у них решение для защиты данных.

### Передовая защита

McAfee Web Protection включает в себя технологии обнаружения угроз на нескольких уровнях, обеспечивая таким образом передовую защиту от угроз «нулевого дня» и неизвестных угроз. Использование единой платформы с разными технологиями позволяет McAfee Web Protection оптимизировать систему безопасности. Именно этого требуют многие организации для реализации своих стратегий многослойной защиты. Функция глубокой проверки содержимого позволяет сканировать на наличие скрытых вредоносных программ файлы в форматах ZIP и PDF, а также в графических форматах. Решения веб-защиты компании McAfee были удостоены высших оценок независимых экспертов за точное обнаружение и блокирование до 99 процентов вредоносных программ.

- Интеграция с McAfee Endpoint Security, McAfee Advanced Threat Defense, McAfee Cloud Threat Detection, McAfee Threat Intelligence Exchange, McAfee Cloud Data Protection и McAfee Cloud Visibility — Community Edition.

### Полная защита входящего и исходящего трафика

- Модуль политик на основе правил с бесконечно широкими возможностями настройки обеспечивает выполнение принятых в любой организации правил использования Интернета.
- «Многослойная» система безопасности обеспечивает мгновенную и эффективную защиту от вредоносных программ и других скрытых угроз.
- Фильтрация мобильного трафика для удаленных пользователей ноутбуков и устройств на базе Apple iOS и Google Android.
- Тысячи средств контроля за облачными приложениями.

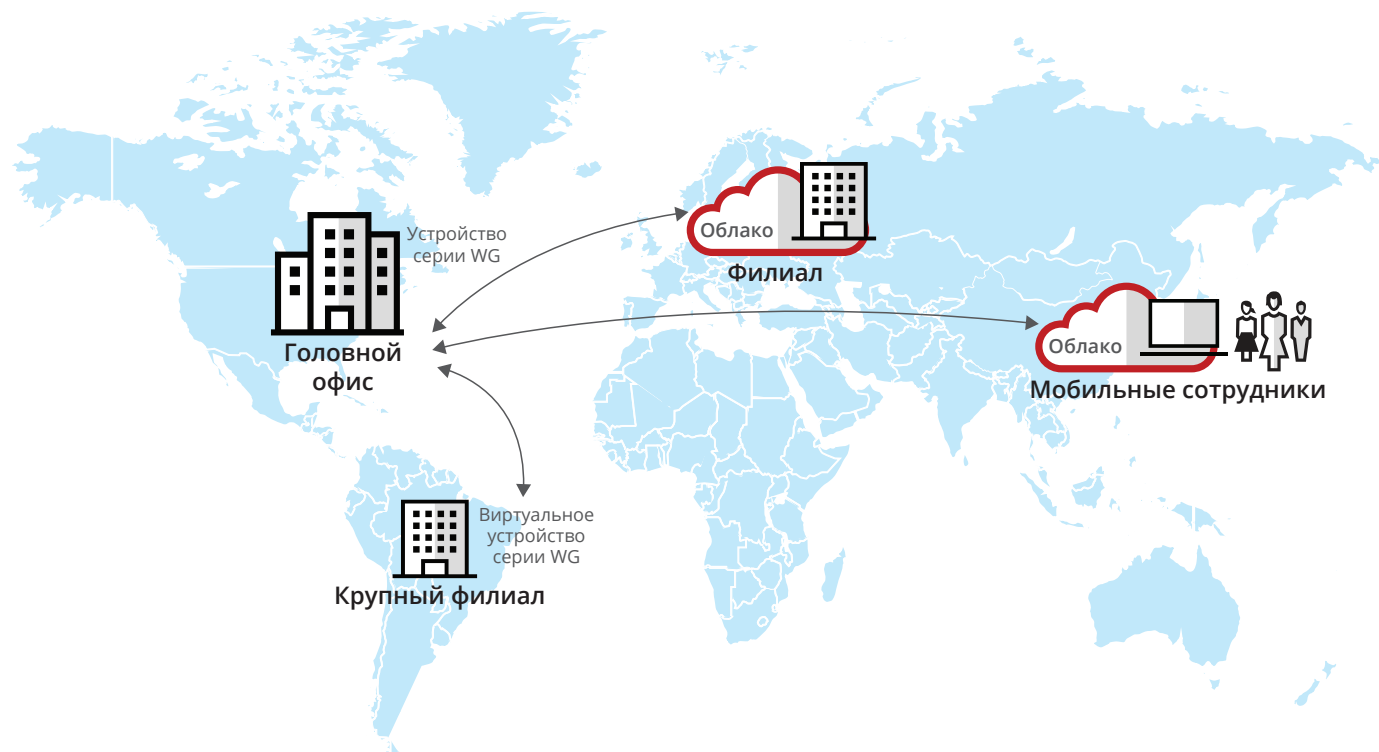


Рис. 1. Решение McAfee Web Protection обеспечивает максимальную гибкость развертывания. Решение может быть развернуто несколькими способами: локально — в виде аппаратных устройств; в виртуальной среде; в облаке; или в виде комбинированного решения, позволяющего сделать процесс развертывания более гибким и обеспечить высокую доступность защиты. Выбор за вами!

Наша передовая многослойная система защиты предлагает следующие возможности:

- **Комплексная антивирусная защита на основе сигнатур с отсылкой запросов в режиме реального времени.** Передовые средства обнаружения вирусов и технология McAfee Global Threat Intelligence (McAfee GTI), позволяющая проверять репутацию файлов в режиме реального времени, дают нам возможность ликвидировать

временной разрыв между моментом обнаружения вируса и моментом обеспечения защиты систем.

- **Анализ репутации веб-сайтов и их классификация с помощью McAfee GTI.** McAfee Web Protection имеет усовершенствованные функции веб-фильтрации и веб-защиты, в которых используется эффективное сочетание методов фильтрации как на основе репутации, так и на основе категорий. В основе средств фильтрации

## Меняющаяся картина угроз

Веб-угрозы сегодняшнего дня отличаются большим многообразием и распространяются самыми разными способами — через ссылки в нежелательных и фишинговых электронных сообщениях, вредоносную рекламу, социальные сети и на первый взгляд безобидные файлы, которые ваши сотрудники используют ежедневно. McAfee Web Protection обеспечивает всестороннюю защиту вашего предприятия.

- От 70 до 90 процентов образцов вредоносных программ обнаруживаются только в одной организации и нигде больше.
- Специалисты McAfee Labs выявляют более 300 новых экземпляров вредоносного ПО в минуту, т. е. примерно пять в секунду.<sup>1</sup>

1. McAfee Labs

## ЛИСТ ДАННЫХ

веб-сайтов, используемых в решении McAfee Web Protection, лежит технология McAfee GTI. Эта технология создает описание всех интернет-объектов (веб-сайтов, адресов электронной почты и IP-адресов) на основе сотен различных атрибутов, получаемых лабораторией McAfee Labs с помощью средств широкомасштабного сбора данных по всему миру. После проверки объектам присваивается репутационный рейтинг исходя из представляемого ими риска, что позволяет администраторам выполнить детальную настройку правил для разрешения или запрещения веб-трафика. Далее технология продолжает выполнять мониторинг этих объектов. Функция динамической классификации содержимого анализирует содержимое неизвестного ранее веб-сайта и определяет, попадает ли он в одну из категорий нежелательных веб-сайтов (азартные игры, порнография, игры и др.).

- **Средство анализа поведения, позволяющее упреждать угрозы «нулевого дня» путем проверки содержимого в режиме реального времени.** В McAfee Web Protection используется запатентованный метод защиты от вредоносных программ «нулевого дня», позволяющий встраивать информацию, получаемую с помощью технологий машинного обучения, в процесс осуществляемой в режиме реального времени (по мере прохождения веб-трафика) эмуляции поведения. Сканируя активное содержимое веб-страницы и имитируя его поведение, а также прогнозируя его намерения,

McAfee Web Protection обеспечивает упреждающую защиту от угроз «нулевого дня» и целенаправленных атак, еще до того, как они попадут на конечные точки.

### Контроль за облачными приложениями

Одним из следствий перехода к использованию облачных приложений является растущая опасность того, что сотрудники будут использовать несанкционированные, «теневые» ИТ-ресурсы. Не отслеживая несанкционированные облачные приложения, специалисты в области информационной безопасности, тем самым подвергают свою организацию опасности утечки данных и финансовых потерь. McAfee Web Protection дает возможность сбора информации обо всем веб-трафике и включает в себя тысячи средств контроля за облачными веб-приложениями, позволяя управлять доступом или ограничивать доступ на основе таких коммерчески важных критериев, как профиль пользователя и связанный с приложением уровень риска.

### Повсеместная защита

Учитывая, что степень распределенности и мобильности персонала постоянно повышается, все большее значение приобретают средства фильтрации веб-содержимого и защиты от веб-угроз, обеспечивающие автоматическое переключение между офисным и мобильным режимами работы. Для защиты и контроля веб-доступа пользователей, находящихся за пределами сети, клиенты могут использовать агент McAfee Client Proxy, интегрированный в McAfee Web Protection и McAfee Endpoint Security.

## ЛИСТ ДАННЫХ

Автоматически обнаруживая наличие шлюза, он направляет веб-трафик либо в локальное, либо в облачное развертывание McAfee Web Protection (в зависимости от местонахождения пользователя), где обеспечивается полное принудительное применение политик. Благодаря интеграции с продуктами наших партнеров AirWatch и MobileIron, разрабатывающих средства управления мобильными устройствами, организации могут обеспечить защиту мобильных устройств на базе Apple iOS и Google Android с помощью той же самой политики веб-защиты, которая используется в отношении всех других устройств в их экосистеме.

### Унифицированная отчетность

Для генерирования отчетов в McAfee Web Protection используется программное обеспечение McAfee® ePolicy Orchestrator® (McAfee ePO™) — широко распространенная и получившая высокие оценки экспертов платформа управления корпоративной безопасностью. В качестве единого источника сводной информации платформа McAfee ePO помогает быстро обнаруживать и устранять проблемы, а также улучшать процесс управления нормативно-правовым соответствием. Для генерирования подробных отчетов о состоянии веб-трафика в McAfee ePO используется модуль McAfee Content Security Reporter.

McAfee Content Security Reporter дает организациям возможность сводить воедино данные, поступающие с платформ McAfee Web Protection, развернутых локально и в облаке, создавая тем самым единую инфраструктуру отчетности. Модуль предоставляет нужную информацию и инструменты, необходимые для понимания того, как в вашей организации используется сеть Интернет, а также для выполнения нормативно-правовых требований, определения тенденций, выявления проблем, учета неприемлемых действий в сети, настройки параметров фильтрации с целью применения ваших политик использования сети Интернет. Модуль дает возможность отображать информацию на панели мониторинга, проводить глубокий анализ веб-трафика и использовать мощные средства автономной обработки данных: все необходимое предлагается в виде одного простого в использовании решения. Для снижения нагрузки на имеющийся сервер McAfee ePO модуль McAfee Content Security Reporter использует внешний автономный сервер, на котором выполняются ресурсоемкие функции обработки и хранения данных. Это дает такой уровень масштабируемости, который позволяет крупнейшим международным корпорациям выполнять требования по отчетности.

Для получения подробных сведений посетите наш сайт [www.mcafee.com/ru/products/web-protection.aspx](http://www.mcafee.com/ru/products/web-protection.aspx).



McAfee Ireland Ltd.  
Building 2000, City Gate  
Mahon, Cork, Ireland  
[www.mcafee.com/ru](http://www.mcafee.com/ru)

McAfee, логотип McAfee, ePolicy Orchestrator и McAfee ePO являются товарными знаками или зарегистрированными товарными знаками компании McAfee, LLC или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Copyright © 2017 McAfee, LLC. 3641\_1017  
Октябрь 2017 г.