McAfee SaaS Web Protection

Комплексная Интернет-безопасность на основе облачных технологий для безопасной и защищенной сети

Интернет открыл дверь для неограниченных возможностей бизнес-деятельности. Как для вашего бизнеса, так и для бизнеса киберпреступников. Каждое Интернет-соединение представляет собой путь для проникновения инфекции, просачивания вредоносных программ и для корпоративного риска. Применив средства оценки рисков, обновляемые программным продуктом McAfee Global Threat Intelligence на ежедневной и круглосуточной основе, McAfee® SaaS Web Protection предлагает легкий, функциональный способ жизненно важной защиты от динамических вредоносных Интернет-атак. Под руководством экспертов по безопасности облачных технологий вы получаете эффективный и экономичный контроль над всеми угрозами и нежелательным доступом в Интернет.

Основные преимущества

- Постоянное обновление защищает всю сеть, даже пользователей роуминга, от быстро изменяющихся вредоносных и шпионских программ, а также фишинга
- Применяет политики относительно работы в Интернет и обеспечивает полную картину работы в сети посредством детальных отчетов по группе пользователей
- Свыше 100 категорий содержимого позволяют гибко его контролировать с целью защиты вашего бизнеса от всевозможных нарушений, которые влекут ответственность перед законом
- Заменяет предсказуемую, легко масштабируемую подписку для растущих потребностей в используемом компанией капитальном оборудовании и персонале
- На смену неуверенности приходит проверенная защита: SaaS Web Protection уже обеспечивает безопасность работы в Интернете более чем 2 000 клиентских организаций, насчитывающих более 100 000 пользователей

Ключевые мотиваторы

- **Вредоносное ПО**
  Общее количество вредоносных программ, собранных за 2007 г.: 5,8 млн; за 2009 г.: 33,3 млн; совокупный темп годового прироста составил 146%
- **Интернет**
  Вредоносных URL за 2006 г.: 173 983; за 2009 г.: 4 261 353; совокупный темп годового прироста составил 190%

Источник: McAfee Labs

Динамическое содержимое и интерактивность Веб 2.0 способствуют повышению количества изощренных угроз из Интернета, ускользающих от обнаружения с помощью традиционных мер защиты. Чтобы защитить своих сотрудников, клиентов, сеть и интеллектуальную собственность, вашей организации необходима проактивная Интернет-защита. Это означает, что вам необходимо решение, не просто блокирующее «известные плохие» URL-адреса, но также и неизвестные, скрытые атаки, смешанные угрозы и шпионские программы.

Свободный доступ к веб-приложениям может также понизить производительность работы пользователей и привести к нарушениям закона. Обеспечение безопасного, правильно организованного доступа в Интернет может привести к большим затратам ресурсов в любой компании, однако если этого не делать, можно столкнуться с тяжелыми последствиями.

McAfee SaaS Web Protection обеспечивает непревзойденную Интернет-безопасность посредством надежной автоматической модели развертывания защиты в качестве услуги (Security-as-a-Service). Не существует более простого и эффективного способа подключения компании к сети Интернет, чем обеспечение при этом ее интерактивной защиты.

Услуга SaaS Web Protection работает быстро, внедряется просто, не требует установки программного или аппаратного обеспечения. Кроме того, нулевая задержка, лучшие в отрасли результаты по времени безотказной работы и масштабируемость в пределах предприятия позволяют обеспечивать производительность и надежность, которая вам необходима для защиты даже самых требовательных и распределенных сред.

Если на предприятии уже внедрена Веб-фильтрация, наша служба – отличный способ добавить защиту от вредоносных программ или реализовать безопасность филиалов и мобильных пользователей.

Полноценная защита входящего и исходящего трафика

Наша услуга SaaS Web Protection обеспечивает всестороннюю защиту трафика Веб 2.0. Она позволяет внедрить политику использования Интернета в организации, автоматически применяя правила доступа к Интернет-трафику, который контролируется политикой. Трафик, не соответствующий политике, блокируется перед входом в сеть. К разрешенному трафику SaaS Web Protection применяет сложные технологии анализа его природы, а также намерений всего содержимого и активного кода на запрошенных веб-страницах. Она мгновенно применяет защиту против вредоносных программ и прочих эксплойтов.

Автоматическая защита обновляется в режиме реального времени

Веб-сайты и их содержимое часто меняются, а киберпреступники научились скрывать свое местоположение и действия. Традиционной блокировки статического URL уже недостаточно. Сеть McAfee Global Threat Intelligence собирает данные в реальном времени от 100 миллионов сенсорных устройств и коррелирует свои действия с учетом ключевых направлений угроз, включая электронную почту, Веб, уязвимости, вторжения на узел и в сеть. Свыше 400 специалистов-исследователей угроз из McAfee Labs™ разработали расширенные средства анализа и службы отслеживания репутации, чтобы делать выводы о намерениях и рисках, а также принимать меры по вашей защите.

Интернет-угрозы и вредоносное содержимое охватывают весь мир, а значит, исследование тоже должно проводиться в глобальных масштабах.

- В Северной Америке URL-адреса нежелательной почты составляют 41% всех Интернет-угроз, за ними следуют вредоносные сайты и сайты с подозрением на вредоносность.
- В пределах Европы, Ближнего Востока и Африки по 31% приходится на нежелательную почту и фишинг, еще 29% – на вредоносные сайты.
- В Латинской и Южной Америке 36% вредоносных URL-адресов связаны с рассылкой нежелательной почты, 30% — припадает на фишинг-сайты и 25% — на прочие вредоносные веб-сайты.
- В Азиатско-Тихоокеанском регионе размещается 31% сомнительных сайтов — их сервера зарегистрированы таким образом, что сайт требует непосредственного мониторинга; URL-адреса нежелательной почты составляют следующую большую группу, насчитывающую 29%, после них идут вредоносные сайты – 24%.

— McAfee Threats Report, Fourth Quarter 2009 (отчет компании McAfee об угрозах, IV квартал 2009 г.), стр. 15

Анализ содержимого с целью обнаружения изменяющихся вредоносных программ

Вредоносные программы на веб-сайтах могут без каких-либо видимых признаков закачивать на машины ничего не подозревающих посетителей и устанавливать клавиатурные шпионы, которые передают такую информацию своему хозяину, сообщая имена пользователей, данные о них, или зомбируют компьютеры, присоединяя их к глобальной бот-сети. Сканируя активное содержимое веб-страниц и определяя его намерения или предсказуемое поведение, мы осуществляем проактивную защиту от неизвестных вредоносных программ, комбинированных угроз, фишинга и целенаправленных атак. Помимо этого, мы можем не допустить нежелательное или запрещенное содержимое, например, порнографию.

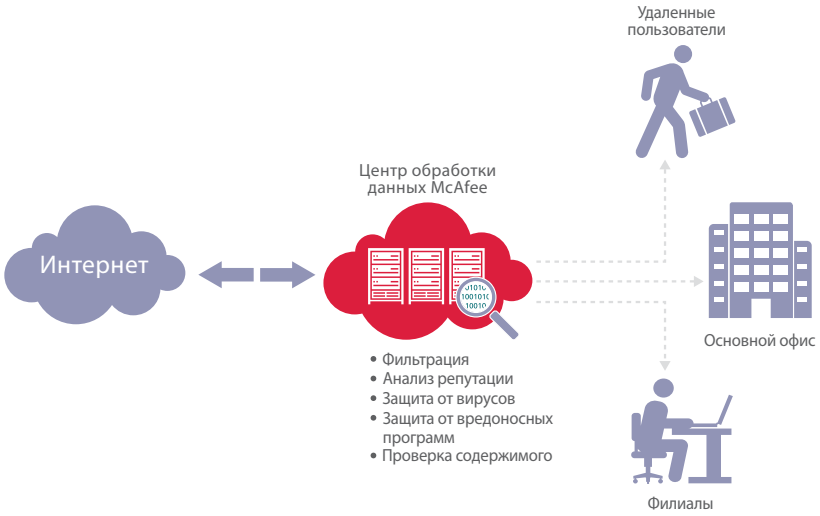
Гибкий контроль на основании категорий и пользователей

Категории упрощают задание политик, направленных против агрессивного, нежелательного и неэффективного использования Интернета. Имея 100 категорий на выбор, предлагаемая нами фильтрация веб-приложений является непревзойденной по гибкости, точности и безопасности. Она предоставляет легкий контроль над неприемлемым использованием Интернета, снижающим производительность или влекущим за собой ответственность перед законом.

Кроме того, для более узко нацеленного контроля категории можно сопоставлять с сообществами пользователей и с содержимым. Например, сайты обмена видео, активно использующие широкополосный канал, могут в пиковое бизнес-время блокироваться для всех, кроме персонала отдела маркетинга. В обеденный перерыв группам поддержки пользователей можно разрешить доступ к сайтам новостей и покупок, но не к игровым порталам. Такой детальный контроль более эффективен, чем огульное блокирование доступа в Интернет; он способствует эффективной и безопасной работе в Интернете.

С нашей безопасностью экономия становится стандартом

Кроме экономии, полученной в результате нашей активной борьбы с вредоносными программами и ограничения доступа к сайтам, содержащим риски, вы снижаете затраты и накладные расходы на ИТ, связанные с очисткой и заменой инфицированных компьютеров. Также контроль навигации и доступа освобождает сетевой канал для необходимой работы, выключая сетевые обновления, снижающие производительность работников.



Функция	Преимущество
Интернет-защита на базе облачных технологий	Сокращает потребности в денежных средствах, постоянные расходы и время, затрачиваемое на управление, тем самым предоставляя службе ИТ возможность заниматься проектами, имеющими ценность для бизнеса.
Достоверная фильтрация на основе репутации	Динамические обновления политики на основе, анализа учитывающего последние сведения.
Активная Интернет-безопасность	Сканирование содержимого веб-сайтов в реальном времени, позволяющее защитить от известных и неизвестных угроз.
Прозрачная идентификация пользователей	Незаметное автоматическое внедрение политик
Сжатие содержимого	Уменьшает требования к пропускной способности и улучшает производительность.
Детальные политики	Правила, созданные в соответствии с потребностями и требованиями работников.
Интеграция с Active Directory или LDAP	Упрощает управление политиками путем эффективного использования функций, заданных для существующих групп пользователей.

McAfee

Быстрая активация службы при минимальных затратах

Security-as-a-Service предлагает наиболее экономичный способ внедрения и поддержания эффективной защиты Интернета. Просто перенаправьте свой Интернет-трафик в наши датацентры со сбалансированной нагрузкой, в которых он будет просканирован с помощью передовых технологий защиты. Интернет-трафик автоматически направляется в ближайший датацентр, емкость и производительность которого позволяют мгновенно обрабатывать все запросы. В результате пользователи выполняют навигацию безопасно без ощутимых задержек.

Поскольку наши эксперты заботятся как об аппаратном, так и о программном обеспечении, вы можете запуститься и быстро работать практически без предварительных вложений. Последующие затраты малозначительны и предсказуемы. Не требуя установки на своих серверах оборудования, клиентских компонентов или обновлений, требующих управления, вы также экономите на ИТ-администраторах, освобождая персонал и бюджет для других необходимых нужд в сфере ИТ. Наше решение масштабируется под потребности самой требовательной среды и поддерживает все стандартные Веб-технологии и обозреватели.

В качестве подписной услуги McAfee постоянно поддерживает защиту и периодически расширяет защитные функции, все это делая прозрачно, безо всякого влияния на ваш бизнес. Команда поддержки McAfee готова ежедневно и круглосуточно отвечать на вопросы пользователей, касающиеся учетной записи и оплаты за услуги по бесплатной телефонной линии или в интерактивном режиме.

Удобное администрирование и отчеты

Настраиваемые панели мониторинга помогают всем администраторам отслеживать тенденции и лучше понимать, как организация использует веб- и почтовые ресурсы. Из любого обозревателя вы можете решить проблему, запротоколировать несанкционированную деятельность, обеспечивать выполнение нормативных требований, выполнять тонкую настройку фильтрации с целью применения политик использования Интернета. Настроенные уведомления предупреждают пользователей о нарушениях политик и блокировке содержимого веб-сайтов. Административные предупреждения мгновенно сообщают о важных событиях системы безопасности.

Необходимо больше?

Объедините McAfee SaaS Web Protection, McAfee SaaS Email Protection и McAfee SaaS Email Archiving, и вы получите комплексную защиту от смешанных Интернет-угроз и поддержку для растущего объема хранилища электронных писем, а также соблюдения нормативных требований.

Для получения дополнительной информации посетите веб-страницу www.mcafee.com/saas.

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

9385ds_saas-web-protection_0410_fnl_ASD