



McAfee SaaS Email Protection and Continuity

Защита электронной почты, доступность и нормативно-правовое соответствие — залог продуктивной работы компании

Простой способ защиты электронной почты и доступа к ней

Основные функции защиты электронной почты, обеспечиваемые решением McAfee SaaS Email Protection and Continuity

- Фильтрация IP-адресов по периметру и блокирование угроз до того, как они попадут в вашу сеть
- Улучшенная защита от «серой почты», спама и мошенничества
- Многоуровневая проверка на наличие вирусов и червей блокирует 100 % всех известных вирусов
- Защита от атак на электронную почту
- Фильтрация сообщений и вложений; применение политик к исходящим сообщениям и вложениям
- Бесперебойная работа электронной почты
- Управление политиками групп
- Аудит, отслеживание и уведомления о доставке сообщений
- McAfee SaaS Email Encryption (дополнительно)

Вы легко обеспечите безопасность электронной почты с помощью решения McAfee® Security-as-a-Service (SaaS) Email Protection and Continuity. Облачная служба не только блокирует нежелательные сообщения, попытки фишинг-мошенничества, вредоносные программы, «серая почта» и неуместное содержимое электронных сообщений раньше, чем они попадут в вашу сеть, но и принудительно применяет политики к исходящей почте, защищая вашу компанию от угрозы утечки данных. Вы можете положиться на постоянную доступность электронной почты, которая обеспечит вашей организации круглосуточный доступ к электронным сообщениям. Благодаря тому, что вам не нужно покупать аппаратное обеспечение и устанавливать программные средства, вы сможете сосредоточиться на защите своей компании, а не на прогоне приложений. При этом, вы будете получать обновления в автоматическом режиме, что позволит вам обеспечивать защиту от новейших угроз.

Электронная почта сегодня — двигатель производительности. Через серверы любой компании ежедневно проходят тысячи электронных сообщений. Управление безопасностью и доступностью электронной почты является тяжелой задачей, которая отвлекает ИТ-персонал от решения задач, имеющих стратегическое значение для достижения бизнес-целей.

Экономичное, простое в управлении решение для защиты электронной почты

Простое в установке решение McAfee SaaS Email Protection and Continuity в любых обстоятельствах защищает вашу сеть и пользователей от угроз, связанных с входящей и исходящей почтой. Служба Software-as-a-Service (SaaS) всегда включена, всегда актуальна, и при этом не требует дополнительных капиталовложений, времени и ресурсов для своего обслуживания. Благодаря тому, что серверный сервис блокирует нежелательные сообщения и угрозы, исходящие из электронной почты, еще до того, как они внедряются в вашу сеть, существенно снижается нагрузка на ваши почтовые серверы. Это позволяет эффективно

использовать серверные ресурсы и экономно расходовать пропускную способность сети. McAfee предоставляет своим пользователям круглосуточно техническую поддержку мирового уровня. Помощь находится на расстоянии одного телефонного звонка!

Упрощенное администрирование и создание отчетов с помощью веб-интерфейса

Рекомендации специалистов встроены в единую интуитивно понятную консоль управления, разработанную на базе веб-интерфейса. Благодаря этому упрощается управление обновлениями политик электронной почты по всем вашим доменам и офисам, высвобождаются ИТ-ресурсы и снижается совокупная стоимость владения. Администраторы могут конфигурировать и применять политики, включая фильтрацию содержимого и правила для содержимого вложений. Политики могут применяться в глобальном масштабе к пользовательским группам или отдельным пользователям, обеспечивая максимальную гибкость. Подробные отчеты, журналы и карантин дают полную информацию об обнаруженных угрозах.



Доступная управляемая безопасность и непрерывная работа электронной почты

- Не требуется покупать, обслуживать, управлять или обновлять какое-либо оборудование или программное обеспечение
- Не требует вложения стартового капитала
- Не требует платы за установку и обновление продуктов
- Автоматическое включение функции непрерывности и функция синхронизации легко обеспечивают непрерывный доступ к почте
- Простое веб-администрирование
- Доступ к круглосуточной службе поддержки без дополнительной платы
- Сертификация в соответствии со стандартом ISO 27001

Непрерывный доступ к электронной почте защищает вашу деловую репутацию, операции и производительность

- Автоматическое включение службы при обнаружении неполадок
- Доступ к электронной почте, поступившей в период отключения, через защищенный веб-интерфейс
- Все функции электронной почты, включая чтение, создание, ответ, пересылку и удаление
- Интеллектуальная синхронизация сообщений электронной почты после сбоя
- Уведомления об отключениях и системные обновления
- Фильтрация входящих и исходящих сообщений

Надежная и устойчивая инфраструктура

Наша стратегия SaaS для центров обработки данных (ЦОД) включает обслуживание многочисленных ЦОД, расположенных на четырех континентах. Каждый центр данных сертифицирован по стандарту ISO 27001 и обеспечивает стопроцентное резервирование с помощью аппаратуры с активным резервированием (active-active), размещенной на всех уровнях сети, включая брендмауэр, маршрутизатор и переключатель для балансировки нагрузки. Внутри каждого ЦОД мы также предоставляем услуги автоматического мониторинга сети и приложений. Мониторинг позволяет, удаленно наблюдая за действиями сотрудников, отслеживать подозрительные и вызывающие беспокойство оповещения и предупреждения, а специалисты по обеспечению безопасности бдительно наблюдают за системами в режиме 24/7.

Строжайшая защита электронной почты

Превосходная защита от нежелательных сообщений

Система Stacked Classification Framework для выявления спама создана на основе запатентованной технологии. Система использует многослойный анализ для определения вероятности того, что сообщение является нежелательным, независимо от языка. Поскольку у каждой фильтрующей технологии существуют свои уникальные возможности, позволяющие обнаружить конкретные угрозы, включая спам на основе изображений. Комбинация технологий создает наиболее точный и полный в отрасли процесс фильтрации.

Служба репутаций McAfee Global Threat Intelligence (McAfee GTI) проверяет каждое сообщение с целью обнаружения известных и новых угроз, связанных с сообщениями, такими как спам. Проверка выполняется, даже если эти сообщения поступают из заслуживающих доверия источников, например, из зараженной системы какой-либо компании, включенной в «белый список». Подобный рейтинг основан не только на совокупной информации датчиков, которые направляют запросы в облако McAfee, и на анализе, выполненном исследователями и автоматизированными инструментами подразделения McAfee Labs, но также на сопоставлении данных, поступающих с различных направлений угроз: файлов, веб-трафика и сети, позволяющих эффективнее и точнее блокировать и отправлять

в карантин сообщения электронной почты, добываясь при этом максимального уровня быстрого действия.

Фильтрация «серой почты» предохраняет и освобождает ваши почтовые ящики

Нежелательными могут быть обычные массовые рассылки, на которые пользователь когда-то подписался, но которые его больше не интересуют (например, отраслевые рассылки и уведомления). Используя фильтры для отсева «серой почты», администраторы могут установить политики фильтрации «серой почты» для отдельных пользователей или групп и даже разрешить пользователям самим включать эту функцию, чтобы очистить почтовые ящики от нежелательных сообщений.

Надежное многоуровневое сканирование эффективно блокирует вирусы и червей

Решение McAfee SaaS Email Protection and Continuity включает WormTraq, нашу собственную технологию обнаружения угроз. Технология, кроме того, осуществляет поиск вредоносных программ как в теле сообщений, так и во вложениях, используя передовое антивирусное ядро на базе сигнатур, в основе которого лежит технология McAfee GTI. Выполняется также не менее важная, чем блокирование входящих атак, фильтрация исходящих сообщений, направленная на защиту ваших клиентов от вредоносных программ.

Полная масштабируемость решения для защиты вашей организации от крупномасштабных атак через электронную почту

Наше полное решение защищает сеть и важнейшие шлюзы электронной почты от атак через электронную почту, мгновенно блокируя атаки типа «отказ в обслуживании», а также от других атак с использованием SMTP, включая атаки с целью сбора действующих адресов, почтовые бомбы и лавинное заполнение каналов.

Встроенное шифрование транспортного уровня безопасности (TLS) обеспечивает защищенную связь между организациями

Организации, которые нуждаются в более высоком уровне защиты исходящей и входящей электронной почты, могут использовать протокол Transport Layer Security (TLS), который принимает и фильтрует входящие и исходящие сообщения, а также выполняет проверку центра TLS сертификации и доставляет электронные сообщения через защищенный канал.

Совместимо с Microsoft Office 365 и Google Apps for Business

Дополнительная информация

Подробную информацию об экономии времени, повышении производительности и уровня защиты, достигаемых в результате применения всех наших решений SaaS, включая McAfee SaaS Email Protection and Continuity, вы найдете на странице www.mcafee.com/ru/products/security-as-a-service/index.aspx.

Постоянный доступ к электронной почте при любых обстоятельствах

Сбой в работе электронной почты еще не означает прекращения работы компании. Решение McAfee SaaS Email Protection and Continuity обеспечивает круглосуточную связь между сотрудниками компании, клиентами, партнерами и поставщиками в период, когда сеть недоступна в результате стихийных бедствий, отключений электропитания или даже из-за штатного техобслуживания. Безопасный и легкий в использовании веб-интерфейс дает пользователям возможность отправлять и получать сообщения, которые всегда будут защищены, искать и извлекать сохраненные сообщения, а также управлять и сообщениями, помещенными на карантин, и банками сообщений.

Включает готовые правила, функцию усовершенствованной проверки содержимого и технологию цифровых отпечатков документов (document fingerprinting)

В вашем распоряжении находится усовершенствованная система предотвращения утечки данных (DLP, Data Loss Prevention) и возможности обеспечивать нормативно-правовое соответствие, что позволяет вам в максимальной степени использовать лучшую в отрасли технологию компании McAfee. Помимо McAfee SaaS Email Protection and Continuity решение McAfee SaaS Email Encryption включает готовые правила для содержимого, отвечающие стандартам защиты информации в индустрии платежных карт (PCI DSS), здравоохранении и финансовой сфере, а также региональным нормативным положениям о конфиденциальности данных и другим нормам. Готовые правила для содержимого позволяют оперативно создавать политики для обеспечения нормативно-правового соответствия. Выполняйте сканирование и обеспечивайте безопасность более 300 типов документов, защищая таким образом свою организацию от утечки исходящих данных.

Усовершенствованная технология идентификации на базе отпечатков документов позволяет создавать и хранить цифровые отпечатки определенных

документов, что позволит «обучить» вашу систему безопасности определять, какой вид содержимого должен быть подвергнут проверке на соответствие установленной политике безопасности. Существует возможность выборочного применения политик на основе найденных в сообщениях и вложениях полных или частичных совпадений с отслеживаемой информацией. Технология поиска по регулярным выражениям может быть также использована для идентификации ключевых слов и фраз.

Простой в использовании механизм шифрования при отправке/запросе данных

Решение McAfee SaaS Email Encryption позволяет вам выполнять шифрование конфиденциальной информации, даже тогда, когда ваш получатель не имеет установленного решения шифрования. Легкая в использовании технология доставки зашифрованных сообщений принудительно и по запросу (push/pull), предназначенная для корпоративных пользователей и осуществляемая даже с мобильных устройств, защищает ваши данные от любопытных глаз.

Оптимизация защиты, управления и нормативно-правового соответствия с помощью технологии Security Connected

Возможность объединения всех решений упрощает управление и связывает воедино все решения защиты, позволяя сократить до минимума время обучения, а также получать всю информацию в режиме реального времени через единую консоль. Управление полным комплектом решений SaaS компании McAfee возможно с единой консоли.

Время перемен

Узнайте о том, как вы можете сократить до минимума объем обслуживания и высвободить свои сверхзагруженные ИТ-службы для решения более важных стратегических задач. Узнать больше о продукте и подписаться на бесплатную ознакомительную версию можно на сайте www.mcafeesaas.com.



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

Intel и логотип Intel являются зарегистрированными товарными знаками Intel Corporation в США и/или других странах. McAfee и логотип McAfee являются товарными знаками или зарегистрированными товарными знаками корпорации McAfee, Inc. или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Планы выпуска продуктов, спецификации и описания, приведенные в настоящем документе, предоставляются только в информационных целях и могут подвергаться изменениям без предварительного извещения; они поставляются без предоставления гарантии какого-либо вида, явной или подразумеваемой. Copyright © 2014 McAfee, Inc. 60166ds_saas-protect-continuity_0313B_fnl_ETMG