McAfee DLP Prevent

Применение политик для защиты конфиденциальной информации

Чем больше людей обменивается информацией в электронном виде, тем выше вероятность того, что кто-нибудь непреднамеренно или умышленно перешлет конфиденциальные данные неавторизованному лицу и тем самым подвергнет секретные корпоративные данные риску. Информация может покинуть пределы компании по самым разным каналам, включая электронную почту, веб-трафик, мгновенные сообщения и FTP. Есть сообщения и транзакции, которые являются допустимыми, но их необходимо шифровать для защиты персональных данных. Другие виды сообщений просто недопустимы ни при каких условиях, поэтому передачу таких сообщений необходимо блокировать. Применение нужных политик в нужное время является важным условием обеспечения безопасности данных, нормативно-правового соответствия и защиты интеллектуальной собственности.

Применение политик безопасности к передаваемым данным

В любой компании сотрудники разных подразделений обмениваются между собой данными, используя самые разнообразные приложения и протоколы. Для предотвращения непреднамеренной или умышленной утечки данных необходимо обеспечить упреждающую защиту конфиденциальной информации от выхода за пределы сети и следить за правильным выполнением бизнес-процессов.

McAfee® DLP Prevent обеспечивает применение политик к информации, выходящей за пределы сети по таким каналам, как электронная почта, веб-почта, мгновенные сообщения, вики-сайты, блоги, порталы, протоколы HTTP/HTTPS и FTP, путем интеграции со шлюзами MTA и использования простого протокола передачи почты (SMTP) или

Ключевые преимущества

Использование существующей инфраструктуры

- Защита корпоративной электронной почты путем интеграции со шлюзами MTA (Message Transfer Agent) и использования протокола SMTP с X-заголовками для блокирования, возврата, шифрования, помещения в карантин и перенаправления сообщений.
- Контроль трафика за счет интеграции с веб-прокси по протоколу ICAP (Internet Content Adaptation Protocol) позволяет блокировать недозволенное содержимое в трафике, передаваемом через HTTP, HTTPS, мгновенные сообщения, FTP и веб-почту.

Подписаться

веб-прокси, поддерживающих протокол ICAP. При обнаружении нарушения политики McAfee DLP Prevent дает вам возможность принять ряд мер, к которым относятся шифрование, блокирование, перенаправление, помещение в карантин и пр., чтобы обеспечить соответствие нормативным требованиям, касающимся защиты конфиденциальной информации, а также сократить риск угроз безопасности.

Полная интеграция с программным обеспечением McAfee ePolicy Orchestrator

McAfee DLP Prevent полностью интегрирован с программным обеспечением McAfee® ePolicy Orchestrator® (McAfee ePO™) и продуктом McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint): у них общие средства управления политиками, инцидентами и ситуациями. Программное обеспечение McAfee ePO дает администраторам возможность создать единую политику защиты электронной почты и веб-трафика и провести ее развертывание на конечных точках и в сети. Кроме того, в McAfee DLP Endpoint и McAfee DLP Prevent используется один и тот же модуль классификации, позволяющий реализовать единую политику защиты электронной почты и веб-трафика. Для обеспечения преемственности при создании общих правил защиты веб-трафика и электронной почты используются общие словари и язык регулярных выражений (regex). Благодаря централизации функций управления, решения McAfee DLP позволяют получать необходимую информацию через единую панель мониторинга, помогают повышать производительность работы и сокращать расходы на администрирование.

Мониторинг электронной почты на мобильных устройствах

McAfee® DLP Prevent для электронных сообщений на мобильных устройствах обеспечивает защиту электронной почты на мобильных устройствах путем анализа содержимого сообщений, загружаемых на мобильное устройство. Для перехвата сообщений используется прокси ActiveSync с функциями DLP. Кроме того, решение может перехватывать ActiveSync как на локальном Microsoft Exchange, так и на Microsoft Office 365 Hosted Exchange. Оно управляется с помощью программного обеспечения McAfee ePO и включено в лицензию McAfee DLP Prevent. Решение не требует установки агента на мобильном устройстве. С помощью McAfee DLP Prevent для электронных сообщений компании могут осуществлять мониторинг электронной почты, направленный на обеспечение нормативно-правового соответствия и сбор доказательного материала. Кроме того, решение обеспечивает защиту как управляемых, так и неуправляемых мобильных устройств.

Упреждающее применение политик для всех видов информации

- Защита более 300 уникальных типов содержимого.
- Применение политик к информации, которая известна как конфиденциальная, а также к информации, о конфиденциальном характере которой вы можете ничего не знать.
- Масштабирование с возможностью поддержки сотен тысяч одновременных подключений.

Классификация, анализ и предотвращение утечки данных

- Фильтрация и контроль конфиденциальной информации для защиты от известных и неизвестных рисков.
- Индексирование и применение детально настраиваемых политик безопасности для всех видов содержимого.
- Применение политик, касающихся доступа к внутренним файлам общего пользования во избежание несанкционированного доступа пользователей к информации и хранилищам данных.

Интеграция с веб-прокси и агентами MTA для повышения уровня защиты

McAfee DLP Prevent интегрируется с веб-прокси (с помощью ICAP) и с агентами MTA (с помощью X-заголовков) для выполнения требуемых действий. Выполняя прерывание несанкционированных транзакций на уровне приложений, а не просто путем завершения сеанса TCP (что никоим образом не изменяет поведение приложения), McAfee DLP Prevent тем самым уведомляет исходное приложение о том, что передача данных была отклонена из-за нарушения политики. Это обеспечивает более высокий уровень защиты вашей организации, поскольку McAfee DLP Prevent накапливает информацию о том, что подлежит защите, и блокирует попытки приложения вести себя так, как прежде.

Защита известной и неизвестной конфиденциальной информации

Благодаря способности классифицировать более 300 различных видов содержимого McAfee DLP Prevent помогает обеспечивать конфиденциальность известной вам информации (паспортных данных, номеров кредитных карт и финансовых данных) и определять, какие документы или данные подлежат защите (например, сложнейшая интеллектуальная собственность). McAfee DLP Prevent содержит широкий диапазон встроенных политик, что дает вам возможность проверять все документы или их часть на соответствие комплексному набору правил и тем самым обеспечивать защиту всей вашей конфиденциальной информации, как известной, так и неизвестной.

Настройка представлений и отчетов об инцидентах

Используя программное обеспечение McAfee ePO, вы можете генерировать сводные представления инцидентов безопасности и следующих за ними действий на основе любых двух контекстуальных точек отсчета. Имеется возможность генерировать представления в виде списков, в виде подробных представлений, а также сводных представлений с отслеживанием тенденций. McAfee DLP Prevent содержит также большое количество готовых отчетов, каждый из которых может быть просмотрен и сохранен для последующего использования. Решение позволяет назначать график периодической рассылки отчетов.

Комплексная классификация данных

McAfee DLP Prevent дает вашей организации возможность защитить конфиденциальные данные всех видов, начиная с данных распространенных, неизменных форматов и заканчивая сложной интеллектуальной собственностью, весьма разнообразной по своему характеру. Благодаря сочетанию названных механизмов классификации объектов McAfee DLP Prevent содержит точнейший классифицирующий инструмент,

Спецификации

Пропускная способность системы

Максимальная скорость анализа, индексации и записи содержимого составляет 150 Мбит/с.

Сетевая интеграция

Интегрируется в сеть в качестве внешнего устройства, работающего в канале передачи данных с использованием агентов MTA и веб-прокси, поддерживающих протокол ICAP.

Типы содержимого

Поддерживается классификация более 300 типов содержимого:

- Документы Microsoft Office
- Мультимедийные файлы
- Файлы пиринговой сети
- Исходный код
- Проектные файлы
- Архивы
- Зашифрованные файлы

блокирующий конфиденциальную информацию и обнаруживающий скрытые или неизвестные риски. Механизмы классификации объектов:

- **Многослойная классификация,** охватывающая как контекстуальную информацию, так и содержимое документов иерархических форматов
- **Регистрация документов,** включающая сигнатуры информации, которые отражают процесс ее изменения
- **Грамматический анализ,** определяющий грамматику и синтаксис любых объектов, начиная с текстовых документов и таблиц и заканчивая исходным кодом
- **Статистический анализ,** учитывающий, сколько раз та или иная сигнатура, грамматическая конструкция или биометрическое совпадение встречаются в том или ином документе или файле
- **Классификация файлов,** определяющая типы содержимого независимо от того, какое расширение имеется у файла или архива

Возможность проведения компьютерно-технических экспертиз и настройки правил

Уникальная технология захвата трафика дает вам возможность повысить скорость и эффективность развертывания путем использования собственных архивных данных за прошлые периоды: вам больше не придется работать наугад, проводить месяцы в пробах и ошибках и мириться с нарушениями в работе компании. Это облегчает задачу точной настройки правил DLP (включая классификацию) с учетом постоянно меняющихся потребностей бизнеса. Технология захвата трафика может также содействовать проведению компьютерно-технических экспертиз, служа своего рода «цифровым магнитофоном», позволяющим тщательно расследовать инциденты DLP путем их воспроизведения постфактум. Технология захвата трафика поставляется либо в виде виртуальной среды, либо в виде массива хранения данных (16 ТБ, 2U), подключенного к устройству NDLP 6600 через кабель SAS.

Форм-фактор и варианты аппаратных устройств

McAfee DLP Prevent можно приобрести в виде аппаратного или виртуального устройства. За дополнительной информацией обратитесь к краткому техническому описанию **аппаратного устройства McAfee DLP 6600**.

Поддерживаемые журналы

Поддерживает HTTP, HTTPS, FTP и протоколы обмена мгновенными сообщениями, которые направляются по протоколу ICAP к ICAP-совместимому веб-прокси. За информацией о протоколах, поддерживаемых вашим прокси-сервером, обращайтесь к своему поставщику прокси-сервера. Поддерживает передачу данных через протокол SMTP за счет интеграции с агентами MTA.

Встроенные политики

- Содержит широкий диапазон встроенных политик и правил, отражающих самые распространенные требования, касающиеся нормативно-правового соответствия, интеллектуальной собственности и допустимого использования данных.
- Позволяет полностью подстраивать правила под организационно-хозяйственные требования конкретной организации при помощи базы данных McAfee для захваченного трафика.

McAfee Together is power.

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