

McAfee Data Loss Prevention Monitor

Обеспечение защиты критически важных данных

Сегодня о защите персональных конфиденциальных данных клиентов и сотрудников (паспортных данных, номеров кредитных карт и т. д.) думают практически все. Почти все организации сталкиваются с такими проблемами безопасности как случайные утечки данных, происходящие в результате ошибок сотрудников, потери ноутбуков и пропажи USB-устройств. Ситуация осложняется тем, что утечка или кража данных может произойти во время их передачи по сети или пересылки с помощью таких веб-приложений, как Google Gmail, Yahoo! Mail, программы обмена мгновенными сообщениями и Facebook. McAfee® Data Loss Prevention Monitor (McAfee DLP Monitor) — это решение для предотвращения утечки данных, имеющее высокий уровень быстродействия и способное анализировать всю передаваемую по Интернету информацию, выявляя случаи, когда информация направляется не туда, куда следует. Оно поможет минимизировать объем работы ваших специалистов по безопасности, обеспечить выполнение нормативно-правовых требований и защитить объекты интеллектуальной собственности и другие важные активы.

Передаваемые данные: мониторинг, отслеживание и отчетность

Любой компании независимо от характера ее деятельности нужна возможность контроля за ситуацией, позволяющая с высокой степенью точности обнаруживать конфиденциальную информацию, передаваемую в любой форме через любое приложение, протокол и порт.

Используя McAfee DLP Monitor, вы можете в режиме реального времени собирать информацию о данных, передаваемых по всей вашей сети, отслеживать их и вести отчетность. Таким образом вы будете знать, какая информация передается между вашими пользователями и другими организациями, и как происходит эта передача. McAfee DLP Monitor — это специализированное устройство с высоким

Ключевые преимущества

- **Продукт полностью объединен с McAfee® ePolicy Orchestrator® (McAfee ePO™).** Имеет общие с McAfee DLP Endpoint политики, средства управления инцидентами и ситуациями.
- **Высокая производительность и масштабируемость.** Кластер, поддерживающий до 8 устройств, с пропускной способностью сканирования 6 Гбит/с.
- **Комплексный анализ.** Обнаружение более 300 уникальных типов содержимого, пересылаемого через любой порт и через любое приложение.
- **Удобные встроенные политики.** Содержит широкий диапазон встроенных политик и правил, отражающих самые распространенные требования нормативно-правового соответствия, защиты интеллектуальной собственности и допустимого использования данных.

Подписаться



ЛИСТ ДАННЫХ

уровнем быстродействия, способное определять более 300 видов содержимого, передаваемого через любой порт и по любому протоколу, что дает вам возможность обнаруживать угрозы безопасности ваших данных и принимать меры для защиты своей организации от утечки данных. Кроме того, с помощью функции уведомления пользователей McAfee DLP Monitor может информировать ваших пользователей о случаях утечки данных, что позволяет изменять их поведение без дополнительных усилий.

Сбор и анализ информации в режиме реального времени

Будучи интегрированным в сеть через SPAN-порт или TAP-порт, McAfee DLP Monitor в режиме реального времени выполняет сканирование и анализ сетевого трафика. С помощью 150 готовых правил, охватывающих такие области, как нормативно-правовое соответствие, политика допустимого использования, интеллектуальная собственность и т. п., McAfee DLP Monitor осуществляет полную и частичную проверку документов на соответствие комплексному набору правил (включая детальную проверку на плагиат). Это дает вам возможность обнаруживать в сетевом трафике аномалии любого масштаба.

Обнаружение ранее неучтенных рисков

Благодаря подробной классификации, индексированию и хранению всего сетевого трафика (а не только информации, которая соответствует применяемым в режиме реального времени правилам), McAfee DLP Monitor дает вам возможность быстро использовать

накопленную информацию для определения того, какие данные являются конфиденциальными, как они используются, кто их использует и куда они перемещаются. Кроме того, избирательное изучение и проверка накопленной информации позволяет обнаруживать события повышенной степени риска и точки утечки данных, которые могли остаться незамеченными прежде. А при использовании этого продукта в сочетании с McAfee DLP Discover вы сможете точно устанавливать, в какой точке вашей сети хранятся данные и кто является их владельцем.

Принятие мер на основе отчетов об инцидентах

Проведя сбор, анализ и классификацию трафика с помощью классифицирующей системы, McAfee DLP Monitor сохраняет всю необходимую информацию в проприетарной базе данных. Используя интуитивно понятный поисковый интерфейс, вы можете просматривать комплексные отчеты о вашей информации: кто ее отправляет, куда она направляется и каким образом ее пересылают. Это дает вам возможность определять, где и как происходит утечка информации и какой информации это касается. Владея такой информацией, вы можете начинать устранять эти угрозы с помощью ряда мер по обеспечению нормативно-правового соответствия и защите конфиденциальных данных.

Классификация всех типов данных

McAfee DLP Monitor дает вашей организации возможность сканировать конфиденциальные данные всех видов, начиная с данных распространенных,

Спецификации

- **Пропускная способность системы:** классификация содержимого: до 800 Мбит/с, без выборки
- **Сетевая интеграция:** пассивно интегрируется в сеть при помощи либо SPAN-порта, либо физического ответвления сети (дополнительно)
- **Возможности кластеризации:** кластер, поддерживающий до 8 устройств при производительности до 6 Гбит/с
- **Поддерживается классификация файлов более 300 типов, в том числе:**
 - Документы Microsoft Office
 - Мультимедийные файлы
 - Файлы пиринговой сети
 - Исходный код
 - Проектные файлы
 - Архивы
 - Зашифрованные файлы
- **Имеет обработчики протоколов для:**
 - FTP
 - HTTP
 - IMAP
 - IRC
 - LDAP
 - POP3
 - SMB
 - SMTP
 - Telnet

ЛИСТ ДАННЫХ

неизменных форматов и заканчивая сложной интеллектуальной собственностью, весьма разнообразной по своему характеру. Благодаря сочетанию указанных механизмов классификации объектов McAfee DLP Monitor получает точнейший классифицирующий инструмент, проводящий фильтрацию конфиденциальной информации и выполняющий поиск внутри этой информации с целью обнаружения скрытых и неизвестных рисков.

Механизмы классификации объектов:

- **Многослойная классификация**, охватывающая как контекстуальную информацию, так и содержимое документов в иерархическом формате.
- **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.



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

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

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 © 2018 McAfee, LLC. 4183_1218
Декабрь 2018 г.