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 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

Ключевые преимущества

- Обнаружение и защита конфиденциальной информации
  - Быстрое обнаружение конфиденциальной информации с помощью интуитивно понятной поисковой системы
  - Проведение компьютерно-технического анализа с целью сопоставления текущих и прошлых событий повышенной степени риска, обнаружения тенденций развития риска и выявления угроз
  - Мгновенное создание правил с целью предотвращения того или иного поведения в будущем
- Полная интеграция с программным обеспечением McAfee® ePolicy Orchestrator® (McAfee ePO™).

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.

Ключевые преимущества (продолжение)

- Устройство полностью управляется программным обеспечением McAfee ePO, которое обеспечивает обмен общими политиками и функциями управления инцидентами и ситуациями с McAfee DLP Endpoint, а также позволяет создавать и редактировать сложные правила.
  - Обнаружение содержимого более 300 видов, пересылаемого через любой порт и через любое приложение
  - Классификация сетевого трафика независимо от порта
  - Масштабирование с возможностью поддержки сотен тысяч одновременных подключений

Спецификации

Пропускная способность системы: классификация содержимого: до 200 Мбит/с, без выборки

Сетевая интеграция: пассивно интегрируется в сеть при помощи либо SPAN-порта, либо физического ответвления сети (по выбору)

Поддерживается классификация файлов более 300 типов, в том числе:

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

Классификация всех типов данных

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

Форм-фактор и варианты аппаратных устройств

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

Спецификации (продолжение)

Поддерживаемые протоколы

- Поддерживает все передачи через любой протокол или порт с использованием TCP в качестве транспортного протокола.
- Содержит обработчики для протоколов HTTP, HTTPS, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, веб-почта, Yahoo! Chat, AOL Chat, MSN Chat, ICY, RTSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule и др.

Встроенные политики

- Содержит широкий диапазон встроенных политик и правил, отражающих самые распространенные требования, касающиеся нормативно-правового соответствия, интеллектуальной собственности, допустимого использования данных.
- Позволяет полностью подстраивать правила под 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