McAfee DLP Monitor

Обеспечение защиты критически важных данных

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

Захват и индексация всего сетевого трафика

- Фильтрация и контроль конфиденциальной информации с целью выявления скрытых или неизвестных рисков
- Индексация всех видов содержимого и последующий интеллектуальный анализ проиндексированной информации с целью получения представления об имеющихся у вас конфиденциальных данных и о том, куда они пересылаются
- Мониторинг доступа к внутренним файлам общего пользования

Создание и редактирование сложных правил

- 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

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. Ситуацию осложняет то, что утечка или кража данных может произойти во время их передачи по сети или при их пересылке с помощью таких веб-приложений, как Google Gmail, Yahoo! Mail, программы обмена мгновенными сообщениями и Facebook. McAfee® Data Loss Prevention (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 организации от утечки данных. Кроме того, с помощью функции уведомления конечных пользователей McAfee DLP Monitor может информировать ваших пользователей о случаях утечки данных, что позволяет изменять их поведение без приложения 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.

intel Security

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)

Типы содержимого

Поддерживается классификация файлов более 300 типов, в том числе:

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

Поддерживаемые журналы

- 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 и допустимого и спользования данных.
- Позволяет полностью подстраивать правила под требования конкретной организации при помощи базы данных McAfee для захваченного трафика.

Обнаружение ранее неучтенных рисков

Благодаря подробному классифицированию, 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, 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, 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. Имея эти данные, вы можете начинать устранять эти угрозы путем принятия ряда мер по обеспечению нормативно-правового соответствия и защите конфиденциальных данных.

Спецификации: устройство McAfee DLP 5500

Компонент	Требование
Процессор	2 шестиядерных процессора Intel E5-2620, кэш-память 15 МБ, 2,0 ГГц, Intel QPI со скоростью 7,20 ГТ/с
Память	DDR3, 1 333 МГц, 32 ГБ
Блок питания	2 модуля электропитания по 760 Вт с возможностью «горячей замены»
Жесткие диски	8 жестких дисков, 2 ТБ, 7 200 об/мин, SATA
Сетевая интерфейсная карта	Модуль ввода-вывода Intel, 1 Гбит/с, Ethernet, два порта, медь
IPMI	4 модуля Intel Remote Management Module (AXXRMM4)
Размер продукта	2 стойко-места (2U)

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.
К механизмам классификации объектов относятся:

- **многослойная классификация,** которая охватывает как контекстуальную информацию, так и содержимое документов иерархических форматов;
- **регистрация документов,** включая биометрические сигнатуры информации, отражающие процесс ее изменения;
- **грамматический анализ** с целью определения грамматики и синтаксиса любых объектов, начиная с текстовых документов и таблиц и заканчивая исходным кодом;
- **статистический анализ** для учета того, сколько раз та или иная сигнатура, грамматическая конструкция или биометрическое совпадение встречаются в том или ином документе или файле;
- **классификация файлов** с целью определения типов содержимого независимо от того, какое у файла или архива имеется расширение.

Спецификации: виртуальные машины

McAfee DLP Monitor выпускается в виде виртуального устройства для средств VMware. Ниже представлены минимальные аппаратные требования для виртуального устройства.

Компонент	Требование
Процессор	4 виртуальных ЦП Intel x86
Память	16 ГБ ОЗУ
Жесткие диски	Жесткий диск 1: не менее 100 ГБ для программного обеспечения виртуальной машины Жесткий диск 2: не менее 512 ГБ для виртуального образа DLP
Сеть	4 виртуальные сетевые карты NIC
BIOS	Функция VT должна быть активирована

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