



McAfee DLP Discover

Обнаружение и защита конфиденциальных данных

Ключевые преимущества

Выявление рисков утечки данных

- Проверка информации, находящейся на всех доступных ресурсах
- Обнаружение местонахождения конфиденциальных данных и определение владельца содержимого
- Просмотр всех собранных данных и поиск по ним с помощью интуитивно понятного интерфейса

Политики и индивидуально настраиваемые отчеты

- Возможность выполнять поисковые запросы и составлять правила защиты на основании полученных результатов поиска
- Использование предустановленных политик, касающихся нормативно-правового соответствия, правил корпоративного управления и интеллектуальной собственности
- Регистрация конфиденциальной информации в смежных системах информационной безопасности

Классификация, анализ и устранение утечек данных

- Механизм многовекторной классификации, позволяющий находить и контролировать конфиденциальную информацию

Информация, хранимая в ноутбуках, на файловых серверах общего доступа, в порталах и в системах управления документами, может подвергаться организации риску. Этот огромный объем информации, который исчисляется в терабайтах или даже в петабайтах, подлежит обязательной защите. Задача это непростая, особенно если учесть, что конфиденциальная информация не всегда должным образом помечена. Кроме того, большинство организаций не имеет возможности узнать или проверить, подвержены ли риску их конфиденциальные данные и куда они могли попасть — даже если в организации используются средства управления доступом. Проблема усложняется еще и тем, что конфиденциальные данные обычно состоят из объектов интеллектуальной собственности, которым сложнее дать формальное определение, чем фиксированным типам данных, таким как номера кредитных карт или паспортные данные. McAfee® DLP Discover поможет определить местонахождение ваших конфиденциальных данных, выявить, кто и как их использует, и защитить их от утечки и утери.

Предотвращение утечки конфиденциальных данных

Интеллектуальная собственность и другие информационные активы, такие как исходный код, коммерческие тайны, стратегические бизнес-планы и т. п., имеют критически важное значение для сохранности вашего бренда, общественной репутации и конкурентного преимущества. Защита данных во время их передачи является критически важной задачей, но ваша первая линия обороны должна определять местонахождение конфиденциальных данных и обеспечивать их защиту еще до того, как они будут несанкционированным образом прочитаны или перемещены.

McAfee DLP Discover поможет вам защитить вашу организацию от утечки данных. В отличие от прошлых решений, которые требовали от вас предоставления точной информации о том, какое содержимое вы собираетесь

защищать, McAfee DLP Discover обеспечивает полный охват информации, характер которой очевиден, и помогает обнаруживать информацию, характер которой не очевиден.

Определение информации, подлежащей защите

Для определения рисков, связанных с информацией и ее распространением, McAfee DLP Discover может быть настроен на поиск информации в заданных хранилищах и на обнаружение данных, явно подлежащих защите. Кроме того, все собранные с помощью McAfee DLP Discover данные индексируются, и к ним предоставляется доступ через интуитивно понятный интерфейс, что дает вам возможность быстро проводить поиск потенциально конфиденциальных данных, чтобы знать, кто является владельцем той или иной информации и где она хранится.

Ключевые преимущества (продолжение)

- Индексация всего содержимого и последующий поиск по содержимому с целью обнаружения конфиденциальных данных
- Регистрация и генерирование сигнатур для защиты документов и содержащейся в них информации даже в случае плагиата или перемещения информации
- Отправка предупреждающего сообщения в случае, если содержимое документа нарушает правила безопасности

Спецификации

Типы содержимого

Поддерживается классификация файлов более 300 типов, в том числе:

- Документы Microsoft Office
- Мультимедийные файлы
- Исходный код
- Проектные файлы
- Архивы
- Зашифрованные файлы
- Встроенные политики
- Интеллектуальная собственность

Поддерживаемые репозитории

- Common Internet File System (CIFS) / Server Message Block (SMB)
- Network File System (NFS)
- HTTP/HTTPS
- FTP/FTPS
- Microsoft SharePoint
- EMC Documentum
- Базы данных: Microsoft SQL, Oracle, DB2, MySQL Enterprise

Назначение политик защиты

Когда вы будете знать, какая информация подлежит защите, McAfee DLP Discover поможет вам должным образом защитить эту информацию. McAfee DLP Discover предлагает интуитивно понятный и единый механизм создания политик, формирования отчетов и управления с целью обеспечения большего контроля над применением вашей стратегии защиты информации к хранимым данным. К основным преимуществам McAfee DLP Discover с точки зрения политик, правил и классификации относятся:

- большое количество готовых встроенных политик, упрощающих работу;
- мощный механизм составления правил, начиная с простых структурированных данных (кредитные карты, паспортные данные) и заканчивая сложной информацией (интеллектуальная собственность);
- упрощенный процесс создания и проверки правил за счет переноса данных анализа результатов поиска в правило безопасности;
- интеграция со смежными векторами информационной безопасности для обеспечения согласованной защиты;
- игнорирование общедоступных документов и текстов, позволяющее избежать генерирования инцидентов при обнаружении подобной неопасной информации.

Сканирование сети на предмет нарушений

Создав политики, вы можете дать McAfee DLP Discover команду планомерно проверять сетевые ресурсы, чтобы выявлять нарушение политик. Наличие гибких средств планирования задач позволяет проводить непрерывные, ежедневные, еженедельные и ежемесячные автоматические проверки.

McAfee DLP Discover автоматически проверяет на предмет нарушения политик все доступные ресурсы, включая ноутбуки, настольные

компьютеры, серверы, хранилища документов, порталы и места передачи данных. Вы можете задавать группы поиска, группируя ресурсы по IP-адресам, подсетям, диапазонам или сетевым путям. Вы можете также сузить пространство поиска, указав конкретные параметры: например, поиск только по папкам «Мои документы» всех пользователей и игнорирование системных папок или поиск только файлов, принадлежащих определенным пользователям или имеющих определенный размер или тип.

Анализ и устранение нарушений

McAfee DLP Discover предотвращает или сводит до минимума распространение конфиденциальных материалов благодаря интегрированному механизму реагирования на инциденты и управления ситуациями. При обнаружении содержимого, нарушающего политики безопасности, McAfee DLP Discover генерирует инциденты и посылает уведомления. Инциденты, созданные в McAfee DLP Discover, можно отправлять в базу данных, позволяющую привлекать к борьбе с нарушениями специалистов из большого числа подразделений компании. Кроме того, наличие панелей мониторинга риска позволяет специалистам по безопасности легко получать информацию о случаях нарушения политик и генерировать отчеты на основе любого интересующего их параметра хранимых данных.

Захват и анализ хранимых данных

Помимо проверки сетевых ресурсов на предмет нарушения политик McAfee DLP Discover также производит индексацию всего содержимого, обнаруженного на носителях информации в сети, и дает вам возможность анализировать эту информацию, чтобы получить представление об имеющихся у вас конфиденциальных данных. McAfee DLP Discover дает вам возможность быстро получить представление о ваших конфиденциальных данных, о способах их использования, а также о том, кому они принадлежат, где они хранятся и куда они были переданы.

Регистрация документов

Возможна регистрация документов из любого хранилища. Сигнатуры зарегистрированных документов могут либо использоваться локально для определения местонахождения конфиденциальных материалов, либо предоставляться в распоряжение других устройств McAfee, предназначенных для предотвращения утечки данных.

Отчетность

Мощный аналитический механизм, обеспечивающий визуальное представление инцидентов и результатов поиска, позволяет генерировать сводные представления на основе любых двух контекстных точек отсчета. Имеется возможность генерировать представления в виде списков, подробные представления и сводные представления с отслеживанием тенденций. В систему включено более 20 готовых и настраиваемых отчетов

Классификация сложных данных

McAfee DLP Discover 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. Сопоставляя информацию, получаемую с помощью указанных механизмов классификации объектов, McAfee DLP Discover в состоянии создать точнейшую многовекторную классификацию, которая используется для фильтрации и контроля конфиденциальной информации, а также для поиска внутри этой информации, позволяющего обнаруживать скрытые и неизвестные риски. 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;

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 (AXXRM4)
Размер продукта	2 стойко-места (2U)

- **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: устройство McAfee DLP 5500

McAfee DLP Discover 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 интерфейсные карты
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

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 © 2013 McAfee, Inc. 60417ds_dlp-discover_0813B