McAfee Data Loss Prevention Discover

Обнаружение, классификация и защита конфиденциальных данных независимо от места их хранения

Ключевые преимущества

Выявление рисков утечки данных

- Сканирование информации, хранящейся локально и в облаке
- 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

Конфиденциальная информация любой организации, хранимая на ноутбуках, файловых серверах общего доступа и в облачных хранилищах, является для данной организации потенциальным источником риска. 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 помечена должным образом. 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 осложняется еще и тем, что конфиденциальные данные обычно состоят из неструктурированных данных (например, из объектов интеллектуальной собственности). А дать формальное определение неструктурированным данным сложнее, чем структурированным (к последним относятся, например, номера кредитных карт, паспортные данные и т. п.). McAfee® Data Loss Prevention (DLP) Discover помогает находить и классифицировать конфиденциальные данные, определять, как они используются, и защищать их от кражи и утечки.

Какие изменения произошли в McAfee DLP Discover?

McAfee DLP Discover теперь может сканировать и защищать данные, находящиеся в облачном хранилище Box. Для централизованного управления данным решением используется программное обеспечение McAfee ePolicy Orchestrator® (McAfee ePO™), позволяющее легко создавать необходимые политики и автоматизировать сканирование данных по заранее составленному графику. Есть возможность генерировать особые отчеты об инцидентах и получать подробную аналитику.

intel Security

Классификация, анализ и устранение утечек данных

- Механизм многовекторной классификации, позволяющий находить и контролировать конфиденциальную информацию
- 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:

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

Основные функции:

- Программный вариант McAfee DLP Discover позволяет отказаться от использования аппаратных и виртуальных устройств и тем самым дополнительно сократить расходы.
- Развертывание решения и управление им полностью осуществляется с помощью программного обеспечения McAfee ePO. McAfee DLP Discover дает возможность использовать то же самое расширение управления и ту же самую политику DLP, что и в DLP Endpoint.
- Полная совместимость с функциями классификации данных в DLP Endpoint.
- Совместимость с Windows Server 2008 и Windows Server 2012.
- Поддерживает распределенные варианты развертывания, позволяющие использовать невостребованную пропускную способность имеющихся серверов и охватывать большие географической области.
- Лицензия совместима с аппаратными устройствами DLP Discover версий 9.3.x и с программным вариантом DLP Discover версии 9.4.

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 и узнать, кто является владельцем той или иной информации и где она хранится.

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);

Поддерживаемые репозитории

- Common Internet File System (CIFS) / Server Message Block (SMB)[1]
- Network File System (NFS)
- HTTP/HTTPS
- FTP/FTPS
- Microsoft SharePoint[1]
- EMC Documentum
- Базы данных: Microsoft SQL, Oracle, DB2, MySQL Enterprise

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.

- 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.

Спецификации: Программный вариант

McAfee DLP Discover можно приобрести в виде программного (неаппаратного) варианта. Ниже представлены минимальные требования к системе.

Аппаратные требования

- Центральный процессор: Intel Core 2, 64-разрядный
- Оперативная память: не менее 4 ГБ
- Свободное место на диске: не менее 100 ГБ

Поддерживаемые платформы

- Windows Server 2008 R2 Standard (64-разрядная версия)
- Windows Server 2012 Standard (64-разрядная версия)
- Windows Server 2012 R2 Standard (64-разрядная версия)

Поддерживаемые системы виртуализации

- vSphere ESXi 5.0, обновление 2
- vCenter Server 5.0, обновление 2

Программное обеспечение и агенты McAfee ePO

- McAfee ePO версии 4.6.8 или более поздней версии; McAfee ePO версии 5.1 или более поздней версии
- McAfee Agent версии 4.8.2 или более поздней версии; McAfee Agent версии 5.0 или более поздней версии

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 используются для фильтрации и контроля конфиденциальной информации, а также для поиска внутри этой информации, позволяющего обнаруживать скрытые и неизвестные риски. Имеются следующие механизмы классификации объектов:

- Многослойная классификация, охватывающая как контекстуальную информацию, так и содержимое документов иерархических форматов
- 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

Спецификации: устройство McAfee DLP 5500

McAfee DLP Discover можно приобрести в виде физического или виртуального устройства. Ниже приведены спецификации аппаратного устройства.

Компонент	Описание
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)

Спецификации: виртуальные машины

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 карты NIC
BIOS	Функция VT должна быть активирована

1. Программная версия McAfee DLP Discover 9.4 на данный момент поддерживает CIFS, Microsoft SharePoint 2010 и Microsoft SharePoint 2013.

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