McAfee DLP Prevent

Применение политик для защиты конфиденциальной информации

Ключевые преимущества

Использование существующей инфраструктуры

- Защита корпоративной электронной почты путем интеграции со шлюзами MTA и использования протокола SMTP с X-заголовками для блокирования, возврата, шифрования, помещения в карантин и перенаправления сообщений
- Контроль трафика благодаря интеграции с веб-прокси, поддерживающими протокол ICAP, что дает возможность блокировать недозволенное содержимое в трафике, передаваемом через HTTP, HTTPS, мгновенные сообщения, FTP и веб-почту

Упреждающее применение политик для всех видов информации

- Защита содержимого более 300 типов файлов данных
- Применение политик к информации, про которую вы знаете, что она является конфиденциальной, а также к информации, про которую вы можете ничего не знать
- Масштабирование с возможностью поддержки сотен тысяч одновременных подключений

Чем больше людей обменивается информацией в электронном виде, тем выше вероятность того, что кто-нибудь непреднамеренно или умышленно перешлет конфиденциальные данные неавторизованному лицу и тем самым подвергнет конфиденциальные корпоративные данные риску. Электронная почта, веб-трафик, мгновенные сообщения, FTP — информация может покинуть пределы компании по большому числу разных электронных каналов. Есть сообщения и транзакции, которые являются допустимыми, но их необходимо шифровать для защиты персональных данных. Есть такие виды сообщений, которые не приемлемы ни при каких условиях, поэтому передачу таких сообщений необходимо блокировать. Применение нужных политик в нужное время является важным условием обеспечения безопасности данных, нормативно-правового соответствия и защиты интеллектуальной собственности.

Применение политик безопасности к передаваемым данным

В любой компании сотрудники разных подразделений обмениваются между собой данными при помощи большого числа разных приложений и протоколов. Для предотвращения непреднамеренной или умышленной утечки данных необходимо обеспечить упреждающую защиту конфиденциальной информации от выхода за пределы сети и следить за правильным выполнением бизнес-процессов.

McAfee® Data Loss Prevention (DLP) Prevent обеспечивает применение политик к информации, выходящей за пределы сети по таким каналам, как электронная почта, веб-почта, мгновенные сообщения, вики-сайты, блоги, порталы, HTTP/HTTPS и FTP, путем интеграции со шлюзами MTA (Message Transfer Agent) и использования простого протокола передачи почты (SMTP) или веб-прокси, поддерживающих протокол ICAP.

При обнаружении нарушения политики McAfee DLP Prevent дает вам возможность принять ряд мер, к которым относятся шифрование, блокирование, перенаправление, помещение в карантин и пр., чтобы обеспечить соответствие нормативным требованиям, касающимся защиты конфиденциальной информации, и сократить риск угроз безопасности.

Интеграция с веб-прокси и агентами MTA для повышения уровня защиты

McAfee DLP Prevent интегрируется с веб-прокси (с помощью ICAP) и с агентами MTA (с помощью X-заголовков) для выполнения требуемых действий. Выполняя прерывание несанкционированных транзакций на уровне приложений, а не просто путем завершения сеанса TCP (что никоим образом не изменяет поведение приложения), McAfee DLP Prevent тем самым уведомляет исходное приложение о том, что передача данных

intel Security

Ключевые преимущества (продолжение)

Классификация, анализ и предотвращение утечки данных

- Фильтрация и контроль конфиденциальной информации с целью выявления известных или неизвестных рисков
- Индексирование и применение тонко настроенных политик безопасности для всех видов содержимого
- Применение политик, касающихся доступа к внутренним файлам общего пользования, чтобы пользователи не могли получить несанкционированный доступ к информации или хранилищам данных

Спецификации

Пропускная способность системы
Максимальная скорость анализа, индексации и записи содержимого составляет 150 Мбит/с.

Сетевая интеграция
Интегрируется в сеть в качестве внешнего устройства, работающего в канале передачи данных с использованием агентов MTA и веб-прокси, поддерживающих протокол ICAP.

Типы содержимого
Поддерживается классификация файлов более 300 типов:

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

была отклонена по причине нарушения политики. Это обеспечивает более высокий уровень защиты вашей организации, поскольку McAfee DLP Prevent накапливает информацию о том, что подлежит защите, и блокирует попытки приложения вести себя так, как прежде.

Защита известной и неизвестной конфиденциальной информации

Благодаря способности классифицировать более 300 различных видов содержимого McAfee DLP Prevent помогает обеспечивать конфиденциальность известной вам информации (паспортных данных, номеров кредитных карт и финансовых данных) и определять, какие документы или данные подлежат защите (например, сложнейшая интеллектуальная собственность). McAfee DLP Prevent содержит широкий диапазон встроенных политик, что дает вам возможность полностью или частично проверять документы на соответствие комплексному набору правил и тем самым обеспечивать защиту всей вашей конфиденциальной информации, как известной, так и неизвестной.

Настройка представлений и отчетов об инцидентах

Используя консоль управления McAfee® ePolicy Orchestrator® (McAfee ePO™), вы можете генерировать сводные представления инцидентов безопасности и следующих за ними действий на основе любых двух контекстуальных точек отсчета. Имеется возможность генерировать представления в виде списков, подробные представления и сводные представления с отслеживанием тенденций. McAfee DLP Prevent содержит также большое количество готовых отчетов, каждый из которых может быть просмотрен, сохранен для последующего использования или запланирован для периодической рассылки.

Комплексная классификация данных

McAfee DLP Prevent 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. Благодаря сочетанию указанных механизмов классификации объектов McAfee DLP Prevent имеет точнейший классифицирующий инструмент, блокирующий конфиденциальную информацию и обнаруживающий скрытые или 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;
- **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 (продолжение)

Поддерживаемые журналы

Поддерживает HTTP, HTTPS, FTP и протоколы обмена мгновенными сообщениями через протокол ICAP к веб-прокси, поддерживающему ICAP. За информацией о протоколах, поддерживаемых вашим прокси-сервером, просим обращаться к поставщику вашего прокси-сервера. Поддерживает SMTP через интеграцию с агентами MTA.

Встроенные политики

- Содержит широкий диапазон встроенных политик и правил, отражающих самые распространенные требования, касающиеся нормативно-правового соответствия, интеллектуальной собственности и допустимого использования данных.
- Позволяет полностью подстраивать правила под требования конкретной организации при помощи базы данных McAfee для захваченного трафика.

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)

Спецификации: виртуальная машина

McAfee DLP Prevent 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
Сетевые порты	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