McAfee DLP для защиты данных на пути от устройств до облака

Универсальная защита данных

Переход на использование облачных сервисов, таких как Microsoft Office 365, с целью предоставить сотрудникам бóльшую свободу выбора и легкий доступ к основным бизнес-приложениям наблюдается в компаниях самых разных размеров. Локальные решения для защиты данных, как правило, не имеют доступа к данным в таких облачных сервисах, как Office 365, и не могут контролировать совместную работу или обмен данными в облаке. Многие организации планируют взять на вооружение отдельное решение для защиты данных в облачной среде, но при этом дробят свои политики, отчетность и процесс реагирования на инциденты. Это приводит к увеличению эксплуатационных издержек и непоследовательной практике защиты данных на устройствах, в сетях и в облачных службах.

McAfee® DLP для защиты данных на пути от устройств до облака обеспечивает универсальную защиту данных на конечных точках, в сетях и в облаке благодаря интеграции двух передовых технологий: McAfee® Data Loss Prevention (McAfee DLP) и McAfee® MVISION Cloud. Такая интеграция дает организациям возможность беспрепятственно свести воедино все процессы обеспечения защиты данных, минимизировать риск утечки данных и добиться максимальной производительности труда.

Неэффективность фрагментарных решений для защиты данных

Для реализации решений DLP в облаке раньше требовалась переделка «под облако» правил DLP, созданных для локального контекста. В правилах для локально развернутых систем DLP, кроме того, отсутствовал контекст встроенных в облако средств совместной работы и обмена данными с третьими лицами через облачные службы. Это приводило к чрезмерным затратам времени на дублирование

Ключевые преимущества

Полная интеграция

- Классификация данных один раз в программном обеспечении McAfee ePO и использование полученных классификаций в контексте устройства, сети и облака
- Подключение локальной и облачной систем DLP друг к другу выполняется всего одним щелчком мыши и занимает менее одной минуты

Согласованные процессы предотвращение утечек данных

- Один общий модуль управления политиками и классификациями для работы в разных средах
- Для внесения необходимых изменений достаточно использовать одну-единственную консоль

Подписаться

выполненной ранее работы на устройствах и в сети и непоследовательному применению политик различными модулями DLP. Поэтому утечки данных, причиной которых послужили совместная работа или ссылки общего доступа в облаке, оставались невидимыми для локального решения DLP.

Простота объединения и синхронизации локальной и облачной систем DLP

Программное обеспечение McAfee® ePolicy Orchestrator® (McAfee ePO™) упрощает реализацию системы DLP для защиты данных на пути от устройств до облака. Благодаря взаимодействию программного обеспечения MVISION Cloud и McAfee ePO вы сможете защитить данные в любом облачном сервисе быстрее чем когда-либо, имея при этом полную контекстную информацию о встроенных в облако средствах совместной работы и обмена данными. Подключение двух решений выполняется одним щелчком мыши, занимая менее одной минуты.[1] Правила DLP, встроенные в программное обеспечение McAfee ePO для ваших устройств и сети, передаются решению MVISION Cloud, где могут применяться к любой облачной службе и любому облачному трафику, идущему в обход вашей сети. Классификации ваших данных синхронизируются, обеспечивая согласованное предотвращение утечки данных на конечных точках и в облаке. Информация о всех инцидентах передается программному обеспечению McAfee ePO, благодаря чему у вас будет единый рабочий процесс DLP на всем пути от устройства к облаку.

Как предприятия повышают производительность труда с помощью DLP для устройств и облака

Клиенты, которые приобрели программное обеспечение McAfee ePO, пользуются преимуществами этой интеграции. Они без труда применяют правила DLP в облачных сервисах и упрощают свои производственные операции. Например, крупному поставщику услуг общественного питания, использующему McAfee DLP на конечных точках и в общих сетевых файловых ресурсах, нужно было выяснить, где именно в облаке находятся его данные, и разработать стратегию их защиты. Эта организация начала с анализа своего веб-трафика с помощью McAfee® Web Gateway, чтобы определить наиболее популярные места назначения, выбираемые пользователями, и места хранения данных компании в облаке. В результате организация обнаружила, что бóльшая часть ее данных фактически сосредоточена в Microsoft Office 365.

Требования этой компании к защите данных в облаке не отличались от требований к локальным защитным решениям, но контекстуальные различия, такие как обмен файлами и совместная работа в облаке, создавали проблемы нового характера. Например, компании необходимо было сканировать по требованию данные в Office 365 аналогично сканированию локальных данных, обеспечивая при этом соблюдение правил DLP для данных, перемещающихся в Office 365 и из него, уникальных для облака и не видимых при сборе информации

Ключевые преимущества (продолжение)

Единое представление для всех процессов управления инцидентами и генерирования отчетов

- Централизованное управление инцидентами в разных средах
- Для просмотра инцидентов и отчетов переключаться между консолями не требуется

о происходящем в сети компании. Было установлено, что наилучшим решением, удовлетворяющим этим требованиям, является брокер безопасного доступа в облако (cloud access security broker — CASB), и была проведена оценка нескольких представленных на рынке решений. В конечном итоге эта организация выбрала MVISION Cloud благодаря его тесной интеграции с уже действующими правилами DLP в программном обеспечении McAfee ePO. Специалисты отдела ИБ перенесли локальные классификации данных из программного обеспечения McAfee ePO в MVISION Cloud, а затем написали политики для Office 365, используя эти готовые классификации. Теперь у этой организации есть единое место для управления классификациями данных и инцидентами DLP как с устройства, так и из облака, а также для создания отчетов о веб-трафике с помощью McAfee Web Gateway — и все это представлено в программном обеспечении McAfee ePO.

«Мы выбрали в качестве брокера безопасного доступа в облако решение McAfee MVISION Cloud потому, что оно предоставляет информацию о том, куда передаются наши данные и кто имеет к ним доступ, а также благодаря простоте понимания риска, связанного с использованием облачного сервиса».

— Директор по информационной безопасности международной компании-производителя IoT-устройств

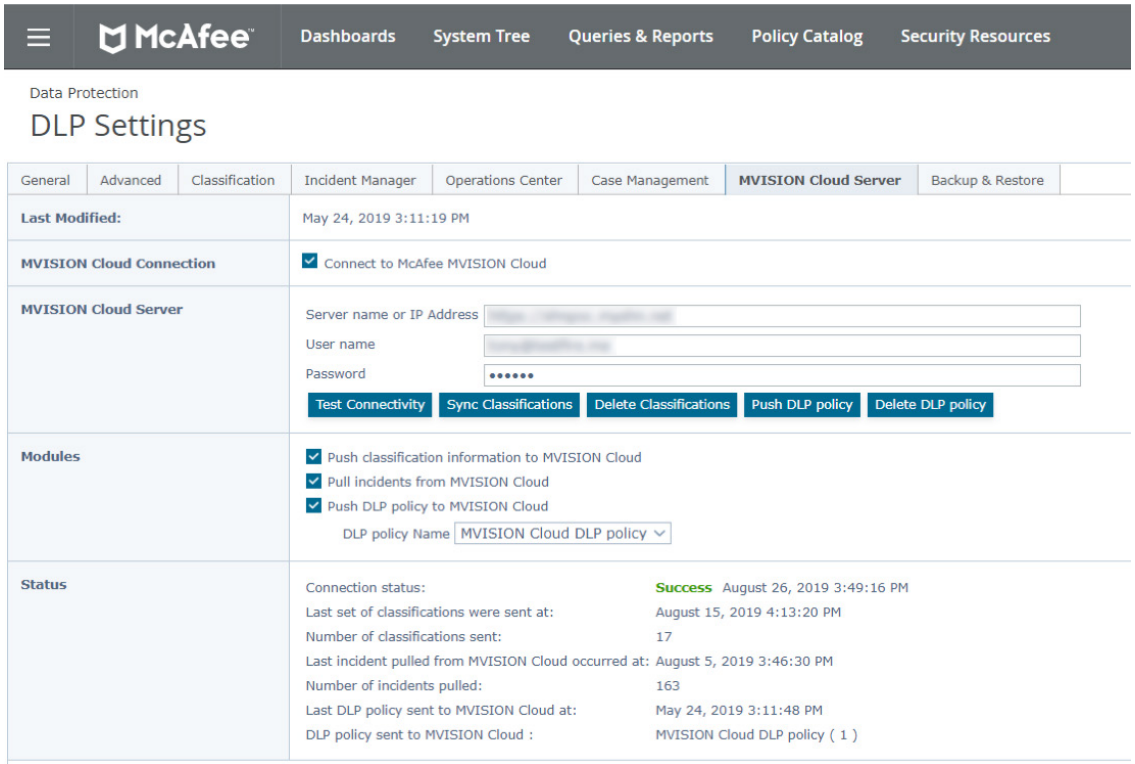

Рис. 1. Синхронизация политик DLP с MVISION Cloud в программном обеспечении McAfee ePO.

Централизованное управление инцидентами и создание отчетов

Приобретая программное обеспечение McAfee ePO, вы получите в свое распоряжение единую консоль для управления всеми нарушениями политик DLP и для генерирования отчетов. Это позволяет вам просматривать инциденты и генерировать отчеты, не переключаясь между консолями, независимо от того, где происходят нарушения DLP: на корпоративных устройствах или в облачных приложениях.

Наличие централизованной консоли, собирающей информацию о конфиденциальных данных в разных средах, помогает также упростить задачу проведения аудитов и обеспечения нормативно-правового соответствия.

Выводы

На фоне роста объемов данных, изо дня в день создаваемых в облаке и отправляемых в облако, крайне важное значение приобретает наличие систематизированного набора политик DLP, обеспечивающих защиту данных по всем векторам утечки данных независимо от того, где эти данные хранятся: на корпоративных конечных точках, на неуправляемых устройствах, в сети или в облачных приложениях.

McAfee DLP для защиты данных на пути от устройств до облака дает организациям возможность обеспечить слаженную универсальную защиту данных в самых разных средах, экономя время за счет повышения производительности труда и минимизируя риск утечки данных.

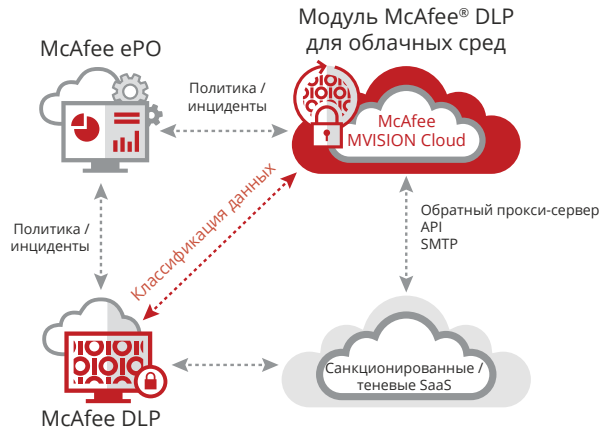

Рис. 2. Общая архитектура управления инцидентами в McAfee DLP для защиты данных на пути от устройств до облака.

Дополнительная информация

Для получения подробной информации посетите страницу **www.mcafee.com/enterprise/ru-ru/products/data-protection-products.html**.

1. По результатам проведенных в McAfee систематических лабораторных испытаний.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru