Решения McAfee для предотвращения потери данных

В: Что такое предотвращение потери данных (DLP)?

О: Решения для предотвращения потери данных (Data Loss Prevention - DLP) помогают организациям защитить конфиденциальную информацию, которая циркулирует и хранится в их сетях. Они позволяют контролировать данные с помощью политик, которые описывают атрибуты, определяющие данные и виды операций, доступные пользователю при работе с этими данными. Решения DLP обычно делятся на две категории: «Легкие DLP», которые, как правило, принимают форму расширенного фильтра содержания документов, встроенного в шлюз безопасности и в продукты для защиты настольных ПК, и «полные DLP», которые отличаются намного большим количеством функций контроля, гибкостью и широкими возможностями, обеспечивая защиту данных в масштабе всей инфраструктуры организации — от USB-диска до межсетевого экрана и далее.

В: Какие задачи решает DLP?

О: DLP защищает конфиденциальные данные. Это относится к данным, которые попадают под действие регулирующих норм, таким как номера кредитных карт, медицинские карты или информация о банковских счетах, а также к интеллектуальной собственности и другой информации, имеющей большую ценность для организации: планам выпуска новой продукции, финансовым отчетам и планируемым приобретениям. Обеспечить защиту такого рода данных не просто, поскольку в процессе работы организации эти данные нужно передавать, хранить и администрировать. DLP применяет средства контроля к такого рода информации, проверяя ее содержание и применяя политики безопасной обработки, обеспечивающие защиту данных с сохранением возможности их санкционированного использования.

В: Для чего нужна система DLP?

О: Если вы храните или обрабатываете регламентированные данные, такие как учетные записи клиентов, номера счетов, номера кредитных карт, медицинские карты и даже личные дела сотрудников, или если вы работаете с конфиденциальными данными компании, такими как финансовые отчеты и конструкторская документация, то у вас есть данные, которые вы либо обязаны защищать, либо хотели бы защитить в своих собственных интересах. Защитить конфиденциальные данные, не имея специализированного комплексного решения, практически невозможно. Вы можете заблокировать свои рабочие станции и ограничить доступ в Интернет, и это поможет защитить некоторые конфиденциальные данные, но значительная их часть останется незащищенной, а производственный процесс замедлится. DLP позволяет защитить данные, сохраняя производительность труда и гибкость бизнеса.

В: Как работает DLP?

О: Решение DLP контролирует данные в покое, в движении и в процессе использования. Применяя анализ с учетом содержания, оно выявляет конкретные элементы данных, соответствующие заранее определенным моделям, которые описывают особенности конфиденциальных данных вашей организации. Оно следит за действиями пользователей по отношению к данным и на основе выработанной компанией политики оценивает, соответствуют ли такие действия этим данным. Если данные используются в нарушение политики, могут быть приняты различные меры уменьшения риска. В число таких мер могут входить замечания, уведомления, мониторинг, шифрование, переадресация, карантин и даже блокирование.

В: Как установить DLP?

О: Большинство решений DLP требуют длительного цикла развертывания: нужно устанавливать серверы, устранять уязвимости операционных систем, устанавливать сторонние базы данных и т.п. Затем нужно привлекать консалтинговые фирмы для продолжительного анализа рисков предприятия, чтобы определить, какие политики ему необходимы. McAfee считает, что существует лучший путь. Наше решение можно внедрить за считанные дни, не месяцы. Это уменьшает сложность и стоимость и значительно сокращает потребность в услугах дорогостоящих консультантов. Наши простые в развертывании программно-аппаратные комплексы можно установить и пустить в эксплуатацию за считанные минуты. Затем мы осуществляем мониторинг использования реальных данных в вашей организации и предоставляем вам эту информацию, чтобы вы могли протестировать политики, прежде чем приступить к их применению. Это исключает циклы метода проб и ошибок, проходимые пользователями других систем, и выявляет охраняемые данные в кратчайшие сроки с минимальными усилиями и максимальной точностью.

В: Будет ли решение McAfee® Data Loss Prevention работать с моими системами электронной почты и веб-безопасности?

О: Да. Сетевые компоненты решения McAfee для предотвращения утечки данных используют отраслевые стандарты. Программно-аппаратный комплекс McAfee DLP Prevent устанавливается вместе с существующими системами электронной почты и интернет-шлюзов и использует протокол SMTP для взаимодействия со шлюзом электронной почты и протокол ICAP_ spelled_out (ICAP) для взаимодействия с прокси-сервером Web. При этом не требуется никакого специализированного программирования или работ по интеграции с существующими решениями.

В: Не предназначена ли DLP только для регулируемых отраслей?

О: Нет. Любая организация, которая имеет дело с конфиденциальными данными любого типа, такими как конструкторская документация, планы сотрудничества или внутренняя финансовая информация, нуждается в защите доступа к этим данным, чтобы сохранить свою репутацию и конкурентные преимущества. Дома вы храните свои ценности в сейфе. На работе нужно так же хорошо заботиться о данных, представляющих большую ценность.

В: DLP лучше, чем шифрование?

О: DLP очень хорошо сочетается с шифрованием. Для достижения статуса «безопасной

гавани» с точки зрения соблюдения нормативных требований может быть достаточно одного шифрования. Тем не менее, оно может стать препятствием для гибкой и отзывчивой работы предприятия. Допустим, вы просто используете шифрование для защиты всех данных на серверах, в настольных ПК и ноутбуках. Если шифрование применяется правильно, он обеспечит защиту данных, хранящиеся в этих устройствах.
У этого подхода есть две проблемы. Во-первых, защищены только те данные, которые хранятся в определенных местах. Отсутствует всякая защита данных, которые передается по электронной почте не в те руки, публикуются на неподобающих вебсайтах или похищаются вредоносным ПО, которое передает их за пределы корпоративной сети. Во-вторых, шифрование всего избыточно, так как многие данные, циркулирующие в сети, не нуждается в таком уровне защиты. К тому же найти нужную информацию становится труднее. Если вам надо подготовить документы в связи с судебным расследованием, а вся необходимая информация зашифрована, соблюдение отведенных судом сроков может оказаться почти невозможным.
DLP усиливает возможности шифрования. Встроенные в DLP средства анализа содержания позволяют контролировать данные в тот момент, когда они покидают зашифрованные хранилища. Это означает, что защита следует за данными, куда бы они ни направлялись. Это важное условие реальной защиты ценных информационных ресурсов. К тому же DLP рационализирует шифрование, применяя его только к тем данным, которые нужно защитить. Это облегчает нагрузку по защите данных, сохраняя бизнес-процессы гибкими и способными реагировать на изменения.

В: Не займет ли установка DLP много времени?

О: Другие решения DLP могут потребовать многих месяцев напряженной работы дорогостоящих консультантов, прежде чем начнут приносить какую-либо выгоду. McAfee применяет принципиально иной подход, сокращая время, необходимое для развертывания решения, всего до нескольких дней. Наши усиленные программно-аппаратные комплексы можно установить и пустить в эксплуатацию за считанные минуты, а невероятно богатая информация, которую мы предоставим вам о реальных данных, циркулирующих в сети, позволит быстро создать точные и эффективные политики и за считанные секунды реагировать на изменения в использовании данных или в правилах.

В: Придется ли мне изменить бизнес-процессы?

О: Нет. McAfee DLP – это модульная и гибкая система, которая вписывается в ваш деловой процесс, а не диктует, как его изменить. Тесная интеграция с другими продуктами защиты данных McAfee позволяет выбирать из многих подходов обеспечения безопасности при работе с информацией. Наша централизованная, основанная на ролях консоль администрирования поддерживает делегирование полномочий контролирующим подразделениям организации и обеспечивает беспрецедентный контроль для поддержки принятия стратегических решений.

В: Придется ли использовать еще одну консоль управления?

О: McAfee стремится уменьшить сложность ИТ-защиты. У нас лучшая в отрасли консоль управления McAfee ePolicy Orchestrator® (McAfee ePO™), которая служит единым центром настройки, контроля и отчетности для всех продуктов защиты McAfee в рамках организации. Консоль McAfee можно использовать для решения всех задач по ИТ-безопасности.

В: Как мне найти все свои данные?

О: Решение McAfee Data Loss Prevention предлагает два превосходных инструмента. В отличие от других производителей, мы не требуем, чтобы вы сообщали нашему решению о каждом передаваемом файле и ресурсе, которые могут содержать данные, нуждающиеся в защите. По нашему опыту, не многие знают, где находятся все конфиденциальные данные в их организации. Мы предоставляем инструменты, способные сканировать сети, серверы, сетевые папки и настольные компьютеры в поисках данных, которые либо обозначены как конфиденциальные, либо соответствуют вашему определению подлежащей защите информации. Это делает обнаружение данных гораздо

менее сложным и более эффективным. Мы используем технологию, которая анализирует все данные, передаваемые по вашей сети. Вам даже не нужно знать о существовании этих данных. Если они соответствуют вашим критериям защиты, технология обнаружения выявит их в режиме реального времени и применит методы защиты, указанные в политике. Так как эта технология «прослушивает» сеть на уровне пакетов, вам не придется беспокоиться о том, в каком приложении они созданы, какой протокол используется для их транспортировки, и на какой порт они подаются. Нашему решению, которое защищает информацию на скорости среды передачи, не требуются никакие из этих деталей.

В: Защитит ли DLP данные не только в корпоративной сети?

О: Некоторые другие решения имеют жесткие ограничения на то, что они могут защитить, когда ноутбук или другое мобильное устройство отключено от корпоративной сети. Они либо применяют ограниченную защиту, либо не защищают такие устройства вообще. И то, и другое неприемлемо, так как приводит к образованию огромной дыры в системе защиты данных. McAfee DLP обеспечивает одну и ту же пуленепробиваемую защиту, независимо от того, где вы работаете с компьютером. Это означает возможность применять мобильные технологии, чтобы освободить работников от ограничений, снижающих производительность труда, и с уверенностью расширить сферу своего бизнеса.

В: Не нарушит ли DLP работу предприятия?

О: Некоторые технологии защиты данных действительно могут замедлять работу. Для их установки требуются огромные усилия, а затем аналогичные трудозатраты нужны для того, чтобы регулярно обновлять их по мере изменения данных, бизнеса и норм, регулирующих изменение данных. Более того, некоторые продукты пытаются заблокировать данные, вместо того, чтобы обеспечить их безопасное использование. Это приводит к разочарованию пользователей, поскольку, занимаясь творческой работой, им приходится тормозить на каждом повороте. McAfee DLP — модульное и гибкое решение, которое быстро реагирует на все изменения в среде обработки данных. Оно допускает быстрое создание новых политик, а его уникальные аналитические инструменты предоставляют беспрецедентные сведения об использовании данных в организации, позволяя вносить необходимые изменения прежде, чем станет известно о возникшей проблеме. С решением McAfee DLP вы раскрепостите свой бизнес, не нарушая его.

В: Где я могу больше узнать о McAfee DLP?

О: О решении DLP от McAfee можно подробнее узнать на веб-сайте (www.mcafee.com) или по телефону <НОМЕР> . Вы можете также обратиться к уполномоченному партнеру McAfee, который поможет решить все проблемы, связанные с защитой данных: <URL>.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

8645faq_dtp_dlp9-customer_0210_ETMG