

McAfee DLP Endpoint

Не станьте героем новой истории о крупной утечке данных

Ключевые преимущества

- **Непревзойденная защита.**
Предотвратите потерю данных везде: на работе, дома и в пути.
- **Комплексное управление устройством.** Создайте подробные фильтры для содержимого; укажите критерии для мониторинга и блокировки копирования данных на съемные устройства.
- **Многоуровневая система защиты.** Обеспечение защиты данных на всех конечных точках вне зависимости от операционной системы и типа устройства.
- **Централизованное управление с помощью McAfee ePO.** Применение архитектуры управления рисками безопасности McAfee с целью предотвращения потери данных.
- **Полный визуальный контроль.** Подтверждение наличия мероприятий, направленных на обеспечение соответствия нормативным и корпоративным требованиям, контролируемым аудитором, руководителями предприятий и акционерами.

Теряете данные, даже не зная об этом? Быть может, прямо сейчас информация о клиентах, интеллектуальная собственность, финансовые данные и сведения о персонале покидают границы вашей компании. Злоумышленники — это не только хакеры, но и ваши собственные сотрудники. Случайная или злоумышленная утечка данных может произойти через обычные каналы, например электронную почту, публикации на сайтах, USB-накопители и печать данных, и может обойтись вам в миллионы.

Остановите потерю данных, пока она не произошла

Ежедневно всё новые компании становятся жертвами серьезных утечек данных из-за злоумышленной и случайной потери информации. Согласно недавно проведенному исследованию, свыше 75 процентов компаний, входящих в список Fortune 1000, стали жертвами случайной или злоумышленной утечки данных. Данные исследования свидетельствуют о том, что более 55 процентов сотрудников каждую неделю копируют конфиденциальные данные на съемные устройства и выносят их из служебных помещений.¹ Ущерб компаний, возникающий в результате нарушения безопасности данных, и расходы на восстановление составляют чрезвычайно крупные суммы. В 2008 году средний размер ущерба составил 6,65 миллиона долларов.²

А можно ли эффективно и просто предотвратить потерю данных? И при этом управлять соответствием государственным нормативным требованиям и отраслевым стандартам? Теперь можно! С помощью решения для мониторинга, аудита и контроля за действиями пользователей при работе с конфиденциальными данными.

Защита данных и нормативно-правовое соответствие

Вы можете обеспечить полный сбор информации и контроль за передачей важнейших данных с помощью решения McAfee® DLP Endpoint. Решение позволяет мгновенно отслеживать и предотвращать потерю конфиденциальных данных на работе, дома или в пути. McAfee DLP Endpoint защищает вашу организацию от рисков финансовых убытков, ущерба бренду, потери клиентов, снижения конкурентоспособности и несоблюдения нормативно-правовых требований.

С помощью McAfee DLP Endpoint можно быстро и легко отслеживать события в реальном времени, централизованно внедрять политики для управления использованием и передачей конфиденциальных данных сотрудниками

и создания подробных отчетов для судебных разбирательств, при этом не нарушая хода повседневной работы предприятия. Защитите свое предприятие от угроз потери данных, возникающих внутри организации, например через электронную почту и системы мгновенных сообщений, запись данных на компакт-диски, публикации на сайтах, копирование данных на USB-накопители и печать данных. Решение позволяет блокировать утечку конфиденциальных данных от попадания в сеть троянов, червей, а также приложений с совместным использованием файлов, которые взламывают личные данные ничего не подозревающих сотрудников.

Защита без сбоев в работе

Решение дает возможность предотвратить потерю и утечку данных, при этом не нарушая законную повседневную работу, даже тогда, когда речь идет о данных, которые были изменены, скопированы, вставлены, сжаты или зашифрованы. С помощью решения вы можете защитить содержимое более 390 типов файлов данных. Уникальные алгоритмы цифровых отпечатков (fingerprinting) и возможности назначения тегов для содержимого (на основе местоположения, приложений, типа файлов, регулярных выражений, ключевых слов и т. д.) предоставляют широкие возможности для защиты данных, которые позволяют обеспечить информационную безопасность компаний.

Упрощенное управление нормативно-правовым соответствием

Простое управление с помощью McAfee ePolicy Orchestrator® (McAfee ePO™) позволяет отслеживать события безопасности и собирать сведения о компьютерных инцидентах для подтверждения наличия мероприятий, направленных на обеспечение соответствия нормативным и корпоративным требованиям, контролируемым аудитором, руководителями предприятий и акционерами. Интеграция решения McAfee DLP Endpoint с программным обеспечением McAfee ePO

Требования к системе

Операционные системы для сервера McAfee ePO.

- Microsoft Server 2003 с пакетом обновлений 1, выпуск 2

Операционные системы для настольных и переносных компьютеров

- Microsoft Windows XP Professional с пакетом исправлений 1 или выше
- Microsoft Windows 2000 с пакетом исправлений 4 или выше

Аппаратные требования

- Процессор: Pentium III 1 ГГц или выше
- ОЗУ: рекомендуется 512 МБ
- Объем места на диске: минимум 200 МБ
- Сетевое подключение: TCP/IP для удаленного доступа

позволяет без труда собирать важные данные об использовании информации, в том числе сведения об отправителе, получателе, метке времени, а также данные, используемые в качестве улики. Одним нажатием кнопки программное обеспечение McAfee ePO позволяет отслеживать события безопасности в реальном времени и создавать подробные отчеты, призванные подтвердить наличие мероприятий, направленных на обеспечение соответствия нормативным и корпоративным требованиям, контролируемым аудиторами, руководителями предприятий и акционерами.

Выигрыш: непревзойденная защита данных

Вы можете обеспечить полный сбор информации и контроль за данными, покидающими конечные точки, и таким образом предотвратить утечки данных, — а заодно и громкие заголовки в СМИ — до их возникновения.

McAfee DLP Endpoint входит в состав решения для полной защиты данных. McAfee Total Protection™ for Data объединяет модуль McAfee DLP Endpoint и модуль McAfee Endpoint Encryption, представляя собой еще более надежное решение для защиты данных.

Функции

Непревзойденная защита

- Контроль за способом отправки конфиденциальных данных пользователями, доступом к ним, за печатью данных, передачей по сети и через приложения, а также путем копирования данных на устройства хранения. Защищает электронную почту, веб-почту, пиринговые приложения, мгновенные сообщения, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, компакт-диски, DVD, принтеры, факс и съемные устройства.
- Возможности применения политик, которые обеспечивает решение McAfee DLP Endpoint, включают:
 - *Мониторинг.* Разрешение передачи данных.
 - *Предотвращение.* Блокирование передачи данных.
 - *Оповещение.* Оповещение администраторов и конечных пользователей.
 - *Шифрование.* Обеспечение шифрования данных перед передачей.³
 - *Карантин.* Помещение на карантинное хранение до момента авторизации.³

Комплексное управление устройствами

- Контроль за конфиденциальными данными и блокирование копирования данных на USB-устройства, флэш-накопители, устройства iPod и другие съемные устройства.
- Укажите и категоризируйте устройства, которые можно использовать, с помощью любого параметра устройства, функционирующего в среде Windows, включающего идентификатор продукта, идентификатор производителя, серийный номер, класс устройства, его название и т. д.

Многоуровневая защита конечных точек

- Установленные на узлах средства защиты предотвращают потерю данных на конечных точках путем отслеживания и блокирования рискованного обращения пользователей с важными конфиденциальными данными.
- При объединении с McAfee Endpoint Encryption решение McAfee Host DLP Endpoint обеспечивает полноценный многоуровневый подход к предотвращению потери данных.

Централизованное управление с помощью McAfee ePO

- Решение предоставляет доступ к централизованным политикам McAfee DLP Endpoint и мониторингу событий с консоли управления McAfee ePO.
- Возможность использования программного обеспечения McAfee ePO для централизованного управления политиками и мониторинга событий.
- Развертывание агентов и их обновление осуществляется с помощью McAfee ePO.
- Интеграция с программным обеспечением McAfee ePO обеспечивает усовершенствованное управление на базе веб-интерфейса и дополнительные возможности для отчетности и аудита.

Полная информация под рукой

- Комплексная отчетность об авариях и мониторинг событий с помощью решения McAfee Host DLP Endpoint обеспечивает сбор всех необходимых данных, таких как: отправитель, получатель, метка времени и данные, используемые в качестве улики, необходимые для правильного анализа, расследования, проверки, ликвидации последствий и управления рисками.



ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

¹ Illuminas 2007, *Threats Within, Volume II: Data Loss Disaster (Угрозы внутри, том II: Катастрофа: Утечка данных)*

² Исследование Института Понемона по цене утечки данных (*Cost of Data Breach Study*), 2008 г.

³ Входит в состав устройства McAfee Data Loss Prevention