

# McAfee Host Data Loss Prevention

Не станьте героем следующей истории о крупной потере данных

Теряете данные, даже не зная об этом? Информация о клиентах, интеллектуальная собственность, финансовые данные и сведения о персонале могут покидать границы вашей компании прямо сейчас. Правонарушители — это не только злоумышленники, ими могут быть и ваши сотрудники. Случайная и злоумышленная утечка данных может произойти через распространенные каналы, такие как электронная почта, публикация на веб-сайтах, USB-накопители и печать. Она может обойтись вам в миллионы.

## Основные преимущества

### Непревзойденная защита

- Предотвратите потерю данных повсюду: на работе, дома и в пути.

### Полноценное управление устройствами

- Создайте подробные фильтры для материалов; укажите критерии для отслеживания и блокирования передачи данных на съемные устройства.

### Многоуровневая защита

- Убедитесь, что данные защищены на всех конечных точках вне зависимости от операционной системы и типа устройства.

### Централизованное управление с помощью ePO

- Используйте архитектуру управления рисками безопасности McAfee с целью предотвращения потери данных.

### Полная визуализация информации

- Демонстрируйте меры внутреннего и внешнего соответствия аудиторам, высшему руководству и другим заинтересованным лицам.

## Предотвратите потерю данных раньше, чем она произойдет

Ежедневно компании становятся жертвами массовой утери данных из-за злоумышленной и случайной утечки информации. Согласно последнему исследованию, свыше 75 процентов компаний, входящих в Fortune 1000, стали жертвами случайной или злоумышленной утечки данных. Согласно последнему исследованию, 55 процентов сотрудников еженедельно используют съемные устройства для переноса конфиденциальных данных с рабочих носителей информации.<sup>1</sup> Ущерб, наносимый компаниям в результате нарушения безопасности данных, и средства, требующиеся для восстановления, поражают воображение. В 2008 году средний ущерб составил 6,65 миллиона долларов США.<sup>2</sup>

Существуют ли эффективные и простые методы предотвращения потери данных? Возможно ли при этом управлять соответствием постановлением правительства и отраслевым нормам? Теперь всё это возможно благодаря решению для отслеживания и проверки действий пользователей с конфиденциальными данными, а также для контроля над ними.

## Защитите данные и обеспечьте соответствие нормативным требованиям

McAfee® Host Data Loss Prevention (Host DLP) предоставит Вам полный контроль перемещения критических данных, позволяя своевременно выявить и предотвратить потерю данных в офисе, дома или в пути. Host DLP защищает организацию от рисков потери финансовых данных, причинения вреда репутации, потери клиентов, снижения конкурентоспособности и несоответствия нормативным требованиям.

С помощью Host DLP можно быстро и с легкостью отслеживать события в реальном времени, централизованно внедрять политики для управления использованием и передачей конфиденциальных данных сотрудниками, а также создавать подробные отчеты для судебных разбирательств, не влияя при этом на повседневную деятельность компании. Решение позволяет защитить компанию от угроз потери данных,

исходящих изнутри нее самой, например от электронной почты и средств мгновенного обмена сообщениями, а также связанных с записью данных на компакт-диски, публикациями на веб-сайтах, копированием на USB-накопители и печатью. Кроме того, можно остановить потерю конфиденциальных данных, инициированную троянами, червями и приложениями для совместного доступа к файлам, взламывающими личные данные сотрудника незаметным для него образом.

## Непрерывность рабочего процесса

McAfee HDLP позволяет предотвратить потерю и утечку данных без нарушения установленной повседневной деятельности, даже если данные были изменены, скопированы, вставлены, сжаты или зашифрованы. Решение обеспечивает защиту содержимого для более, чем 390 типов файлов. Уникальные алгоритмы идентификации и возможности указания тегов для содержимого (на основе местоположения, приложения, типа файла, регулярных выражений, ключевых слов и т. д.) предоставляют широкие возможности для защиты данных, которые позволяют удостовериться в безопасности информации компании.

## Упрощенное управление соответствием требованиям нормативных актов

Простое управление с помощью McAfee ePolicy Orchestrator® (McAfee ePO™) позволяет отслеживать события и собирать сведения о них с целью предоставления аудиторам, членам совета директоров и другим заинтересованным лицам доказательств того, что были предприняты меры для обеспечения соответствия внутренним и внешним нормативным требованиям. Интеграция Host DLP с ePO позволяет с легкостью собирать важные данные об использовании ресурсов, такие как отправитель, получатель, временная отметка и другие факты. После нажатия кнопки ePO начинает отслеживать события в реальном времени и создавать подробные отчеты с целью предоставления аудиторам, высшему руководству и другим заинтересованным лицам доказательств того, что были предприняты меры для обеспечения соответствия внутренним и внешним нормативным требованиям.

1. Illuminas 2007, Threats Within Volume II Data Loss Disaster (Угрозы внутри. Том II. Катастрофа в связи с утечкой данных, Illuminas, 2007 г.)

2. Ponemon Institute's 2008 Cost of Data Breach Study (Исследование цены утраты данных, Ponemon Institute 2008 г.)

**Системные требования**

**Сервер ePO**

Операционные системы

- Microsoft® Windows Server 2003 SP1, 2003 R2

**Настольные компьютеры и ноутбуки**

Операционные системы

- Microsoft Windows® XP Professional SP1 или выше
- Microsoft Windows 2000 SP4 или выше

Аппаратные требования

- Процессор: Pentium III 1 ГГц или выше
- Оперативная память: рекомендуется 512 МБ
- Дисковое пространство: не менее 200 МБ
- Сетевое подключение: TCP/IP для удаленного доступа

**Выигрыш: непревзойденная защита данных**

McAfee Host DLP предоставляет полную информацию о данных, покидающих конечные точки, и установить контроль над ними, чтобы воспрепятствовать их потере и негативным последствиям до того, как они произошли. Host DLP входит в состав решения для полной защиты данных. McAfee Total Protection™ for Data объединяет Host DLP с McAfee Endpoint Encryption, чтобы предоставить еще более полное решение для защиты данных.

**Функции**

**Непревзойденная защита**

- Управление способом отправки конфиденциальных данных пользователями, получения доступа к ним, их печати и передачи по сети через приложения и на устройствах хранения. Защита электронной почты, веб-почты, одноранговых приложений, средств обмена мгновенными сообщениями, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, компакт-дисков, DVD, принтеров, факсов и съемных дисков.
- Возможности применения DLP включают:
  - » Отслеживание - передача данных разрешена.
  - » Предотвращение - передача данных блокируется.
  - » Уведомление - уведомление администраторов и конечных пользователей.
  - » Шифрование - шифрование данных перед передачей.\*
  - » Карантин - ожидание дальнейших действий.\*

\*Выполняется в устройстве McAfee Data Loss Prevention

**Полноценное управление устройствами**

- Управление копированием конфиденциальных данных на USB-устройства, флэш-накопители, iPod и другие съемные устройства и их блокирование при необходимости.

- Определение и категоризация устройств, разрешенных к использованию, с помощью параметра устройства в Windows, включающего идентификатор продукта, идентификатор производителя, серийный номер, класс устройства, его название и т. д.

**Многоуровневая защита для конечных точек**

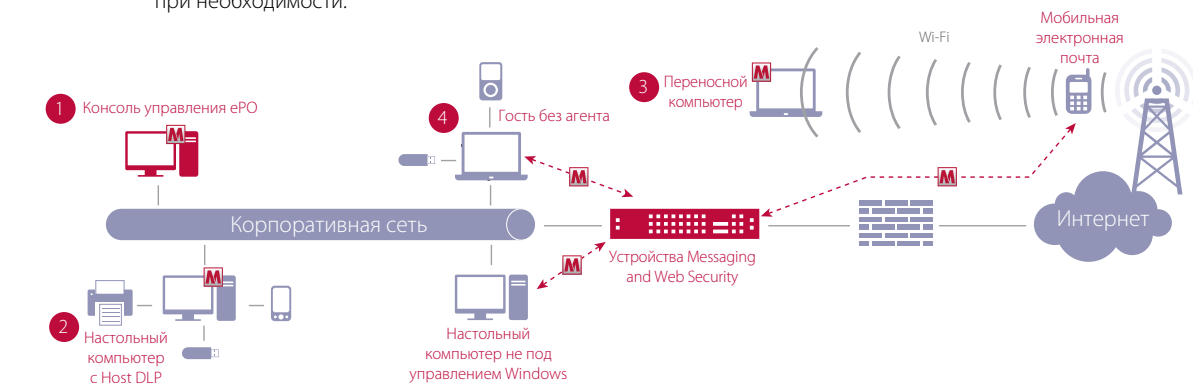
- Серверная защита предотвращает потерю данных на конечных точках путем отслеживания и блокировки рискованного обращения пользователей с важными конфиденциальными данными.
- В сочетании с Endpoint Encryption решение Host DLP обеспечивает полноценный многоуровневый подход к предотвращению утери данных.

**Централизованное управление с помощью ePO**

- Обеспечение доступа к централизованным политикам Host DLP и отслеживанию событий с консоли управления ePO.
- Использование ePO для централизованного управления политиками и отслеживания событий.
- Развертывание агентов и их обновление с помощью ePO.
- Интеграция с ePO 4.0 предоставляет расширенное управление на основе веб-приложения и дополнительные возможности отчетности и проверки.

**Полная информация под рукой**

- Используйте отслеживание событий Host DLP и полноценную отчетность по ним для сбора нужных данных, таких как отправитель, получатель, временная метка и другие факты для правильного анализа, исследования, проверки, ликвидации последствий чрезвычайных ситуаций и управления рисками.



**1 Консоль управления ePO.** Централизованное управление политиками, аудитом, отчетностью и распространением программного обеспечения. Позволяет обеспечить соответствие политик безопасности бизнес-процессам и операциям.

**2 Host DLP и Endpoint Encryption.** Отслеживание, подготовка отчетности, контроль и предотвращение действий пользователей, ставящих данные под угрозу. Надежное шифрование, получившее сертификат FIPS, для целого диска или отдельных файлов и папок защищает целостность данных в случае утери или кражи устройства.

**3 Endpoint Encryption for Mobile.** Создает зашифрованное защищенное пространство на мобильных устройствах, обеспечивая сохранность конфиденциальных данных. Защищает целостность и конфиденциальность данных в случае утери или кражи устройства.

**4 Device Control и Endpoint Encryption.** Контролируем обращение пользователей с внешними устройствами, такими как iPod и USB-накопители, чтобы предотвратить утерю конфиденциальных данных. Надежное полнодисковое шифрование ноутбука гарантирует, что его нельзя будет использовать в случае утери или кражи.



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

McAfee и логотип McAfee являются товарными знаками или зарегистрированными товарными знаками корпорации McAfee, Inc. или ее филиалов в США и других странах. Остальные марки и бренды находятся в исключительной собственности соответствующих владельцев. Планы выпуска продуктов, спецификации и описания, приведенные в настоящем документе, предоставляются только в информационных целях и могут подвергаться изменениям без предварительного извещения; они поставляются без предоставления гарантии какого-либо вида, явной или подразумеваемой. Copyright ©2010 McAfee, Inc. 9726ds\_host-dlp\_0710\_fnl