

# McAfee Total Protection for Data

Всесторонняя защита критичных для деятельности компании данных

Компрометация конфиденциальной информации клиентов неоднократно попадала в новостные заголовки за последние несколько лет. Неоднократно эти данные были вынесены через парадную дверь компании на переносном компьютере или другом мобильном устройстве. Компании, которые испытывают такую потерю данных, рискуют серьезными последствиями, включая штрафы от регулирующих структур, обнародование, вред для торговой марки, недоверие клиентов и финансовые потери. В 2008 году средний ущерб, которые терпели компании вследствие подобных отказов системы защиты, составил 6,65 миллиона долларов.<sup>1</sup>

В современной среде с повсеместным доступом к Интернету и стремительно растущим числом мобильных устройств защита конфиденциальной информации клиента и интеллектуальной собственности должна иметь первоочередный приоритет.

## Основные преимущества

### Предотвращение потери данных

- Применение политик безопасности с центральным управлением для регулирования того, каким образом сотрудники получают доступ к конфиденциальным данным, как используют и передают их.

### Шифрование устройств на уровне предприятия

- Шифрование целого диска в сочетании с надежным контролем доступа для защиты конфиденциальных сведений на всех конечных точках.

### Постоянное шифрование файлов и папок

- Автоматическое, прозрачное и мгновенное шифрование файлов и папок до их передачи по организации.

### Консоль централизованного управления

- Определение корпоративных политик безопасности, контролирующих шифрование, мониторинг и защиту конфиденциальных данных.
- Сокращение времени и усилий, затрачиваемых на управление и обучение, что приводит к увеличению прибыли на инвестированный капитал и снижению общей стоимости владения.

### Расширенные возможности отчетности и регистрация

- Отслеживание событий в режиме реального времени и создание подробных отчетов
- Демонстрация мер внутреннего и внешнего соответствия аудиторам, членам совета и другим акционерам.

## McAfee Total Protection for Data

Чтобы обезопасить ваши конфиденциальные данные, McAfee® Total Protection for Data является наиболее полноценным решением, доступным в отрасли. В нем используется надежное шифрование, проверка подлинности, предотвращение потери данных и управление безопасностью, основанное на политиках, для предупреждения несанкционированного доступа и переноса вашей конфиденциальной информации – где угодно, в любое время.

### Предотвращение потери данных

Предотвращение потери данных начинается с улучшения обзора и контроля над данными, пусть даже скрытых. McAfee Total Protection for Data позволяет вам внедрять и вводить в действие политики безопасности для всей компании, которые регулируют и ограничивают способ использования и передачи вашими сотрудниками конфиденциальных данных по общим каналам, таким как электронная почта, мгновенные сообщения, печать и накопители для USB. Не имеет значения, где находятся ваши сотрудники: в офисе, дома или в дороге. Вы имеете полный контроль.

### Шифрование устройств на уровне предприятия

Обеспечьте безопасность своих конфиденциальных данных благодаря решению защиты на уровне предприятия. Total Protection for Data использует шифрование всего диска в сочетании с надежным контролем доступа через двухфакторную аутентификацию до перезагрузки для предотвращения несанкционированного доступа к конфиденциальным данным на всех конечных точках, включая настольные и переносные компьютеры, КПК, смартфоны и т. д.

### Постоянное прозрачное шифрование файлов и папок

Убедитесь, что ваши файлы и папки постоянно шифруются независимо от того, где данные редактируются, копируются или сохраняются, включая настольные и переносные компьютеры, КПК, смартфоны и т. д. Total Protection for Data выполняет шифрование контента, автоматически, прозрачно и мгновенно шифруя выбранные вами файлы и папки до их перемещения внутри организации. Чтобы ввести в действие шифрование для определенных файлов и папок без взаимодействия с пользователем, нужно создать и внедрить центральные политики, основанные на пользователях и их группах.

### Централизованное управление безопасностью и расширенная отчетность

McAfee Total Protection for Data интегрируется с McAfee ePolicy Orchestrator® (McAfee ePO™), чтобы сократить постоянные затраты на управление, развертывание, отчетность и аудит. Эта интеграция помогает эффективно удовлетворять постоянно меняющимся требованиям к обеспечению конфиденциальности, обеспечивать постоянную защиту и демонстрировать соответствие нормативным требованиям внутренним и внешним аудиторам, а также другим основным акционерам. Помимо обеспечения централизованного, основанного на политиках управления, эта интеграция также обеспечивает расширенные возможности отчетности, что помогает соответствовать жестким требованиям в отношении соблюдения конфиденциальности со стороны правительства и отрасли, гарантирует защиту "Safe Harbor" и демонстрирует соответствие внутренним и внешним аудиторам, членам совета и другим основным акционерам.

<sup>1</sup> Ponemon Institute's 2008 Cost of Data Breach Study.

**Системные требования**

**Сервер ePO**

**Операционные системы**

- Microsoft Server 2003 SP1, 2003 R2

**Аппаратные требования**

- Пространство на диске: 250 Мб
- Оперативная память: 512 Мб1 Гб ОЗУ (рекомендуется)
- Процессор – Intel Pentium II или выше – минимум 450 МГц

**Настольные компьютеры и ноутбуки**

**Операционные системы**

- Microsoft Vista\* (все 32- и 64-битовые версии)
- Microsoft Windows XP Professional SP1 или выше
- Microsoft Windows 2000 SP4 или выше
- \* Доступно для DLP в 2008

**Аппаратные требования**

- Процессор: Pentium III 1 ГГц или выше
- Оперативная память: рекомендуется 512 Мб
- Пространство на диске: минимум 200 Мб
- Сетевое подключение: TCP/IP для удаленного доступа

**Конечные точки: мобильные устройства Windows**

**Операционные системы**

- Microsoft Windows Mobile 6.0 for Smartphone
- Microsoft Windows Mobile 6.0 for PDA
- Microsoft Windows Mobile 5.0 for Smartphone
- Microsoft Windows Mobile 5.0 for Pocket PC

**Аппаратные требования**

- Процессор: минимум 195 МГц
- Оперативная память: 64 Мб
- Сетевое подключение: TCP/IP для удаленного администрирования и ActiveSync 4.5 или выше для установки и обновления через проводное соединение.

**Функции**

**Предотвращение потери данных**

- Управление тем, каким образом пользователи отправляют конфиденциальные данные, получают к ним доступ и производят печать этих данных по сети, через приложения и на устройства хранения: электронная почта, веб-почта, пиринговые приложения, мгновенные сообщения, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, принтеры, факс и съемные диски.
- Прекращение потери конфиденциальных данных, инициированной троянями, червями и приложениями с совместным использованием файлов, взломавшими личные данные сотрудника.
- Защита всех данных, форматов и производных даже при изменении, копировании, вставке, сжатии или шифровании без нарушения законной повседневной деятельности.

**Шифрование устройств на уровне предприятия**

- Полное автоматическое шифрование устройств без необходимости дополнительных действий или обучения конечного пользователя, а также без влияния на ресурсы системы.
- Поддержка шифрования целого диска для нескольких стандартных алгоритмов, включая AES-256 и RC5-1024.
- Идентификация и подтверждение авторизованных пользователей с использованием надежной многофакторной проверки подлинности.

**Постоянное шифрование файлов и папок**

- Файлы всегда остаются зашифрованными, когда они не используются, путем автоматического добавления заголовка файла, перемещаемого с защищенными файлами.
- Файлы и папки всегда защищены при сохранении, включая сохранение на локальных жестких дисках, файловых серверах, съемных носителях и даже в файлах, прикрепленных к сообщениям электронной почты.

**Консоль централизованного управления**

- Использование ePO для указания подробных параметров фильтрации на основе содержимого, мониторинга и блокировке несанкционированного доступа к конфиденциальным данным.
- Управление шифрованием всего диска и шифрованием папок; контроль политики и установка пакетов исправлений; восстановление потерянных ключей; демонстрация соответствия нормативным требованиям.
- Синхронизация политик безопасности с Active Directory, Novell NDS, PKI и т. д.

**Расширенные возможности создания отчетов и регистрации**

- Устройства зашифрованы с расширенными возможностями регистрации.
- Ведется журнал перемещений данных с записью следующей информации: имя отправителя, имя получателя, временная отметка, сведения о данных, дата и время последнего успешного входа в систему, дата и время последнего полученного обновления, запись об успешном или неудавшемся шифровании.

Дополнительную информацию о защите данных можно получить, посетив страницу [www.McAfee.ru](http://www.McAfee.ru).

