McAfee Complete Data Protection — Advanced

Защита данных в любом месте в любое время

Конфиденциальные данные постоянно находятся под угрозой раскрытия, кражи или потери. Не раз и не два конфиденциальные данные были вынесены через парадную дверь компании на переносном компьютере или USB-устройстве. Компаниям, допустившим подобную утечку данных, грозят серьезные последствия, в том числе штрафы от контролирующих органов, необходимость публичного информирования об инцидентах безопасности, ущерб для торговой марки, потеря доверия со стороны клиентов, а также финансовый ущерб. Согласно отчету компании Ponemon Institute, 7 % корпоративных ноутбуков будут рано или поздно потеряны или украдены в период их эксплуатации.[1] Быстрое распространение мобильных устройств с большой емкостью памяти и нередко с доступом в Интернет открывает еще больше каналов для утечки и кражи информации. Именно поэтому защита конфиденциальной, служебной и личной информации должна стать приоритетной задачей. Все эти и многие другие проблемы решаются с помощью комплекта McAfee® Complete Data Protection — Advanced.

Ключевые функции

- McAfee Data Loss Prevention Endpoint
- McAfee Device Control
- Drive Encryption
- File and Removable Media Protection
- Management of Native Encryption
- McAfee ePO Deep Command

Ключевые преимущества

- Контроль за данными путем мониторинга и регламентирования способов использования и передачи сотрудниками конфиденциальной информации по общим каналам, таким как электронная почта, системы обмена мгновенными сообщениями, принтеры и USB-накопители, как на службе, так и за пределами предприятия
- Предотвращение утечки данных в результате действий сложных вредоносных программ, нацеленных на перехват конфиденциальной и личной информации
- Защита данных при их хранении в настольных и переносных компьютерах, в планшетах и в облаке
- Управление встроенными средствами шифрования Apple FileVault и Microsoft BitLocker на конечных точках непосредственно из McAfee ePO

Предотвращение утечки данных для более эффективного контроля

Предотвращение потери данных на конечных точках начинается с улучшения обзора и контроля за данными, даже если они скрыты. Комплект McAfee Complete Data Protection — Advanced позволяет в масштабах всей компании внедрять и принудительно применять политики безопасности, которые регулируют и ограничивают способ использования и передачи сотрудниками конфиденциальных данных по общим каналам, таким как электронная почта, системы обмена мгновенными сообщениями, печать и USB-накопители. Не важно, где находятся ваши сотрудники — в офисе, дома или в пути — они останется под вашим контролем.

Шифрование диска корпоративного класса

Защитите свои конфиденциальные данные с помощью решения корпоративного уровня, отвечающего требованиям стандартов FIPS 140-2 и Common Criteria EAL2+ и ускоренного с помощью набора команд Intel® Advanced Encryption Standard — New Instructions (Intel AES-NI). Для предотвращения несанкционированного доступа к конфиденциальным данным на конечных точках, включая настольные и переносные компьютеры, рабочие станции VDI, USB-устройства, компакт-диски/DVD-диски и пр., комплект McAfee Complete Data Protection — Advanced использует метод шифрования диска в сочетании со строгим контролем доступа посредством двухфакторной аутентификации до перезагрузки.

Шифрование съемных носителей, файлов, папок и облачных хранилищ

Шифрование определенных папок и файлов независимо от того, где происходит изменение, копирование и сохранение данных. Комплект McAfee Complete Data Protection — Advanced выполняет шифрование содержимого, автоматически, прозрачно, «на лету» шифруя выбранные файлы и папки до их перемещения

intel Security

Ключевые преимущества (продолжение)

- Обмен данными и управление конечными точками на уровне оборудования (причем даже выключенными, отключенными и зашифрованными) позволяет избежать вызовов специалистов и бесконечных звонков в службу поддержки при возникновении аварийных ситуаций, вирусных эпидемий или потери паролей шифрования
- Подтверждение соответствия нормативно-правовым требованиям с помощью усовершенствованных инструментов отчетности и аудита; мониторинг событий с составлением подробных отчетов, которые демонстрируют аудиторам и другим заинтересованным лицам соблюдение корпоративных и нормативных требований, предъявляемых к защите конфиденциальной информации

Функции, присущие McAfee ePO Deep Command

- Сокращение времени восстановления систем
- Управление удаленным восстановлением любого ПК в любой точке мира с помощью доступа на аппаратном уровне
- Повышение производительности работы пользователей
- Выполнение ресурсоемких задач в нерабочее время с целью сохранения производительности пользователей
- Снижение расходов на ИТ путем предотвращения частых вызовов специалистов и продолжительных звонков в службу поддержки
- Сокращение эксплуатационных затрат путем реализации программы экономии электроэнергии с сохранением доступа к системам, необходимым для выполнения задач обеспечения безопасности и установки исправлений
- Быстрое обнаружение и подготовка компьютеров с поддержкой технологии Intel vPro AMT путем быстрой идентификации ПК, оборудованных Intel vPro, с последующим включением Intel AMT для быстрой активации

в пределах организации. Чтобы ввести в действие шифрование для определенных файлов и папок без взаимодействия с пользователем, вы можете создавать и централизованно применять политики на базе пользователей и групп пользователей.

Management of Native Encryption

Компонент Management of Native Encryption дает возможность управлять встроенными средствами шифрования томов Apple FileVault в Mac OS X и Microsoft BitLocker в платформах Windows непосредственно из программного обеспечения McAfee® ePolicy Orchestrator® (McAfee ePO™). Management of Native Encryption обеспечивает совместимость с «нулевого дня» с пакетами исправлений и обновлений Mac OS X и Windows, обновлениями микропрограмм Apple, а также поддержку с «нулевого дня» нового оборудования Apple. Management of Native Encryption позволяет администраторам вручную импортировать ключи восстановления томов FileVault и BitLocker, если эти службы активированы пользователями.

Удаленное внеполосное управление снижает эксплуатационные затраты

Программное обеспечение McAfee ePO Deep Command использует технологию Intel® vPro Active Management Technology (Intel vPro AMT), позволяющую сократить эксплуатационные расходы, повысить уровень безопасности и нормативно-правового соответствия и сократить время на дистанционное устранение проблем. Программное обеспечение McAfee ePO Deep Command позволяет вашей компании выводить компьютеры из спящего режима, обновлять политики и безопасно возвращать компьютеры в прежний режим.[2]

Централизованное управление системой безопасности и усовершенствованные инструменты отчетности

Использование единого централизованного программного обеспечения McAfee ePO для внедрения и реализации обязательных к исполнению политик безопасности для всей компании, регулирующих шифрование и мониторинг данных, а также защиту от потери данных. Централизованное определение, развертывание, управление и обновление политик безопасности, обеспечивающих шифрование, фильтрацию, мониторинг и блокирование несанкционированного доступа к конфиденциальным данным.

Функции комплекта McAfee Complete Endpoint Protection — Advanced

Управление устройствами

- Мониторинг и регулирование процессов переноса сотрудниками данных на съемные носители, даже при отсутствии подключения к корпоративной сети

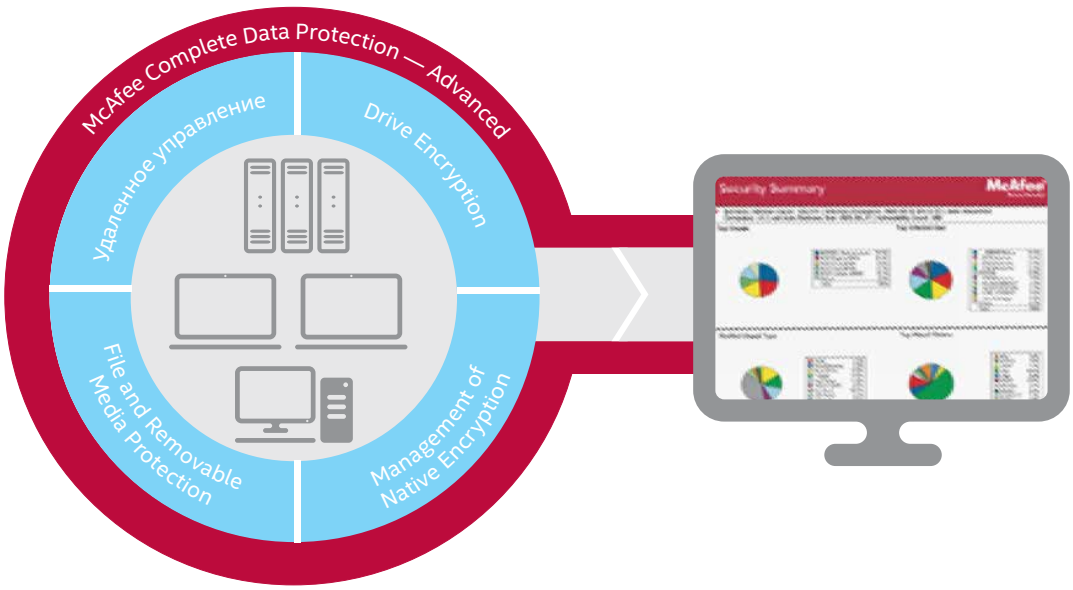

Рис. 1. McAfee Complete Data Protection — Advanced

Спецификации McAfee Complete Data Protection — Advanced

Операционные системы Microsoft Windows

- Microsoft Windows 7, 8 и 10 (32- и 64-разрядные версии)
- Microsoft Windows Vista (32- и 64-разрядные версии)
- Microsoft Windows XP (только 32-разрядная версия)
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 (только 32-разрядная версия)

Аппаратные требования

- Центральный процессор: переносные и настольные компьютеры с Pentium III, 1 ГГц или выше
- Оперативная память: минимум 512 МБ (рекомендуется 1 ГБ)
- Жесткий диск: не менее 200 МБ свободного дискового пространства

Операционные системы Apple Mac

- Mac OS X El Capitan, Yosemite, Mountain Lion и Mavericks

Аппаратные требования

- Центральный процессор: ноутбук Macintosh на основе процессора Intel с 64-разрядным EFI
- Оперативная память: не менее 1 ГБ
- Жесткий диск: не менее 200 МБ свободного дискового пространства

Централизованное управление

- См. техническое описание платформы McAfee ePO.

Спецификации McAfee ePO Deep Command

- Поддержка Intel vPro AMT версий 6.1.2, 7.0, 7.1.4 и 8.0; Intel Setup and Configuration Software (SCS) 8.2

Предотвращение утечки данных

- Управление тем, каким образом пользователи отправляют конфиденциальные данные, получают к ним доступ и выполняют печать этих данных на конечных точках, используя физические и виртуальные устройства, доступ через приложения, а также устройства хранения данных
- Предотвращение утечки конфиденциальных данных, вызванных троянами, червями и приложениями с совместным использованием файлов, которые похищают учетные данные сотрудников
- Защита всех данных, форматов и производных, даже тех, которые были изменены, скопированы, вставлены, сжаты или зашифрованы

Шифрование диска корпоративного класса

- Полное автоматическое шифрование всех устройств, работающее без вмешательства пользователей, не требующее обучения и не отвлекающее на себя ресурсы системы
- Идентификация и проверка авторизованных пользователей путем строгой многофакторной аутентификации

Шифрование съемных носителей

- Автоматическое шифрование в режиме реального времени практически для любых переносных устройств хранения данных — как личных, так и корпоративных
- Повсеместный доступ к зашифрованным данным, не требующий использования дополнительного программного обеспечения

Шифрование файлов, папок и облачных хранилищ

- Данная функция позволяет обеспечивать защиту файлов и папок независимо от того, где они хранятся: на локальных жестких дисках или съемных носителях, в файловых серверах или облачных хранилищах (Box, Dropbox, Google Drive, Microsoft OneDrive и т. п.)

Управление встроенными средствами шифрования на компьютерах Mac и Windows

- Управление томами FileVault на любом оборудовании Mac под управлением Mac OS X Mountain Lion, Mavericks, Yosemite и El Capitan непосредственно из программного обеспечения McAfee ePO
- Управление функциями BitLocker на системах под управлением Windows 7, Windows 8 и Windows 10 непосредственно из программного обеспечения McAfee ePO без необходимости использовать отдельный сервер MBAM (Microsoft BitLocker Management and Administration).

Удаленное внеполосное управление

- Удаленное управление компьютерами на аппаратном уровне за пределами операционной системы
- Возможность включать и пробуждать ПК для выполнения задач по обеспечению безопасности даже в случае его защиты шифром

Центральная консоль управления

- Возможность использовать средства управления инфраструктурой программного обеспечения McAfee ePO для управления шифрованием дисков, папок, файлов и съемных носителей, для контроля политик и управления исправлениями, для восстановления потерянных паролей и для подтверждения нормативно-правового соответствия
- Синхронизация политик безопасности с Microsoft Active Directory, Novell NDS, PKI и др.
- Обеспечение шифрования устройств с широким набором средств аудита
- Ведение журнала перемещения данных для записи информации об отправителях, получателях, отметках времени, сведениях о данных, а также дате и времени последнего успешного входа в систему.

Для получения подробной информации о решениях McAfee для защиты данных посетите наш сайт **www.mcafee.com/ru/products/data-protection/index.aspx**.

1. *The Billion Dollar Lost Laptop Problem Study* (Потеря ноутбука: проблема на миллиард долларов. Исследование), Ponemon Institute, сентябрь 2010 г.
2. *Keep Your Client PCs Safer, Wherever They Go* (Обеспечивайте более надежную защиту персональных компьютеров вашего клиента, где бы они ни находились), **http://www.mcafee.com/ru/resources/solution-briefs/sb-keep-your-client-pcs-safer.pdf**

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com

62238ds_complete-data-adv_0116_fnl