

СУЩЕСТВУЮТ ДВА ОСНОВНЫХ ТИПА ШИФРОВАНИЯ КОНЕЧНЫХ ТОЧЕК:

1

Шифрование всего диска делает ноутбук, сервер или другое устройство непригодным для использования всем, кроме владельцев правильного PIN-кода. Оно защищает операционную систему и данные на ноутбуках и ПК, шифруя весь диск, кроме основной записи загрузки. Она остается незашифрованной, чтобы машина могла загрузить и найти драйвер шифрования для разблокировки системы. Когда компьютер с зашифрованным диском потерян, маловероятно, что кто-то сможет получить доступ к данным на нем. Шифрование всего диска происходит автоматически, поэтому любое содержание, сохраненное на диске, автоматически шифруется.

2

Шифрование файлов, папок и съемных носителей (FFRM) блокирует только определенные файлы или папки. Оно шифрует выбранное содержимое на локальных дисках, сетевых ресурсах или на внешних носителях. Программное обеспечение шифрования использует агенты, шифрующие файлы на основе политик организации. Шифрование на основе файлов поддерживает как структурированные, так и неструктурированные данные, поэтому его можно применять к базам данных, а также документам и изображениям.



TRELLIX DRIVE ENCRYPTION

обеспечивают шифрование, защищающее данные от несанкционированного доступа, потери и разглашения с помощью предварительной аутентификации и мощного шифровального двигателя.

Набор функций Drive Encryption обеспечивает несколько уровней защиты от потери данных со встроенными модулями, решающими конкретные области риска.

ШИФРОВАНИЕ ДИСКА ПОЗВОЛЯЕТ ВАМ:

- ▶ Применять контроль доступа с предварительной аутентификацией.
- ▶ Использовать сертифицированные алгоритмы шифрования (FIPS, Common Criteria).
- ▶ Поддерживать среды с разными устройствами, включая твердотельные накопители.
- ▶ Поддерживать диски с самошифрованием Trusted Computing Group (TCG) Opal v1.0.

Шифрование диска обеспечивает защиту отдельных компьютеров и ноутбуков с системой Basic Input Output System (BIOS) и Unified Extensible Firmware Interface (UEFI).

Политики определяют, как работает программное обеспечение шифрования диска на пользовательском компьютере. Процесс шифрования диска прозрачный для пользователя и почти не влияет на производительность компьютера.

Функции шифрования диска обеспечивают полное шифрование диска для ноутбуков и настольных ПК с ОС Microsoft Windows, а также предотвращают потерю чувствительных данных, особенно в случае потери или кражи оборудования.

- ▶ **Централизованное управление Drive Encryption** полностью интегрируется в Trellix ePO, используя инфраструктуру Trellix ePO для автоматизированной отчетности по безопасности, мониторингу, развертыванию и администрированию политик.
- ▶ **Прозрачное шифрование** — шифрование без помех для пользователей или производительности системы.
- ▶ **Контроль доступа** — Drive Encryption обеспечивает контроль доступа с предварительной аутентификацией.
- ▶ **Восстановление** — позволяет пользователю выполнять аварийное восстановление, когда систему не удается перезагрузить или ее файловая система перед загрузкой (PBFS) повреждена.
- ▶ **Поддержка дисков с самошифрованием** — Drive Encryption и Trellix ePO позволяют централизованное управление самошифрованными дисками, соответствующими стандарту Opal от Trusted Computing Group (TCG), включая блокировку и разблокировку, отчетность, восстановление, обеспечение выполнения политики и управления пользователями.
- ▶ **Доверенный платформенный модуль (TPM)** — Шифрование диска поддерживает TPM 2.0 на системах Windows 8 и более поздних версиях UEFI для обеспечения аутентификации платформы без необходимости предварительной аутентификации (PBA).

TRELLIX FILE AND REMOVABLE MEDIA PROTECTION (FRP)

Trellix FRP обеспечивает автоматическое и прозрачное шифрование файлов и папок, которые хранятся на ПК, файловых серверах, облачных хранилищах, электронной почте и съемных носителях (USB-накопители, CD/DVD и ISO-файлы) или отправляются на них. Trellix FRP убеждает, что определенные файлы и папки всегда зашифрованы, независимо от того, где данные редактируются, копируются или хранятся. Вы можете создавать и обеспечивать централизованные политики на основе пользователей и групп пользователей для определенных файлов и папок без участия пользователя.

Trellix FRP позволяет вам:



Получить доступ к зашифрованным данным в любом месте без какой-либо дополнительной установки программного обеспечения или прав локального администратора на устройстве



Шифровать или блокировать записи на съемных носителях на рабочих станциях VDI



Хранить файлы и папки в безопасности, где бы они ни находились, включая локальные жесткие диски, файловые серверы, съемные носители и облачные хранилища, такие как Box, Dropbox, Google Drive и Microsoft OneDrive

Типичные случаи использования Trellix FRP включают:

- ▶ Шифрование файлов, таких как электронные таблицы и конфиденциальные документы
- ▶ Предоставление доступа к определенной папке в общей сети
- ▶ Шифрование синхронизируемых файлов с облачными хранилищами
- ▶ Шифрование съемных носителей или блокировка копирования незашифрованных файлов
- ▶ Отправка партнерам или клиентам электронных писем с самораспаковывающимися файлами.

ОСНОВНЫЕ ФУНКЦИИ

Функции File and Removable Media Protection обеспечивают шифрование данных на сетевых файлах и папках, съемных носителях, USB-портативных устройствах хранения и в облачных хранилищах.

- ▶ **Централизованное управление** — обеспечивает поддержку развертывания и управления Trellix FRP посредством программного обеспечения Trellix ePO.
- ▶ **Личный ключ пользователя** — для каждого пользователя может быть создан уникальный ключ шифрования.
- ▶ **Делегированное управление через управление ключами на основе ролей** — позволяет логически разделять управление между несколькими администраторами. Эта возможность критическая для разделения функций бизнеса и дочерних предприятий.
- ▶ **Аудит управления ключами и назначение политик** — действия по управлению ключами и назначению политик, выполняемых администраторами Trellix ePO, записываются в журнал аудита. Эта функция критическая для обеспечения соответствия и предотвращения злоупотреблений со стороны привилегированных администраторов.
- ▶ **Защита данных на съемных носителях** — позволяет шифрование съемных носителей и доступ к зашифрованному содержимому даже на системах, где Trellix FRP не установлен.
- ▶ **Защита данных (включая аудит и отчетность) для облачных хранилищ** — позволяет шифровать синхронизированные папки на ПК для Dropbox, Box, Google Drive и OneDrive. Также обеспечивает безопасный доступ к зашифрованным файлам на мобильных устройствах с помощью приложения Trellix Endpoint Assistant.
- ▶ **Шифрование сети** — позволяет обеспечить безопасное совместное использование и сотрудничество на сетевых ресурсах.
- ▶ **Инициирование пользователем шифрования файлов и вложений электронной почты** — позволяет пользователям создавать и добавлять файлы с паролем, которые можно расшифровать на системах, где Trellix FRP не установлен.
- ▶ **Аудит и отчетность событий со съемных носителей USB и CD/DVD/ISO** — записывает все действия пользователей, связанные с событиями со съемными носителями USB и CD/DVD/ISO. Функция аудита предоставляет эффективную обратную связь для администраторов, принимающих решение о политике.
- ▶ **Использование общего криптографического модуля Trellix (MCCM)** — Trellix FRP использует модули пользовательской криптографии и ядра FIPS 140-2 MCCM. Вы можете установить Trellix FRP в режиме FIPS.

