

ІСНУЮТЬ ДВА ОСНОВНІ ТИПИ ШИФРУВАННЯ КІНЦЕВИХ ТОЧОК:

1

Шифрування всього диска робить ноутбук, сервер або інший пристрій непридатним для використання усім, крім власників правильного PIN-коду. Воно захищає операційну систему та дані на ноутбуках і ПК, шифруючи весь диск, крім основного запису завантаження. Він залишається незашифрованим, щоб машина могла завантажити та знайти драйвер шифрування для розблокування системи. Коли комп'ютер із зашифрованим диском втрачено, малоймовірно, що хтось зможе отримати доступ до даних на ньому. Шифрування всього диска відбувається автоматично, тому будь-який зміст, збережений на диску, автоматично шифрується.

2

Шифрування файлів, папок та знімних носіїв (FFRM) блокує лише визначені файли або папки. Воно шифрує вибраний вміст на локальних дисках, мережевих ресурсах або зовнішніх носіях. Програмне забезпечення шифрування використовує агенти, які шифрують файли на основі політик організації. Шифрування на основі файлів підтримує як структуровані, так і неструктуровані дані, тому його можна застосовувати до баз даних, а також документів та зображень.



TRELLIX DRIVE ENCRYPTION

Забезпечує шифрування, яке захищає дані від несанкціонованого доступу, втрати та розголошення за допомогою попередньої аутентифікації та потужного шифрувального двигуна.

Набір функцій Drive Encryption забезпечує кілька рівнів захисту від втрати даних із вбудованими модулями, спрямованими на конкретні зони ризику.

ШИФРУВАННЯ ДИСКА ДОЗВОЛЯЄ ВАМ:

- ▶ Застосовувати контроль доступу з попередньою аутентифікацією.
- ▶ Використовувати сертифіковані алгоритми шифрування (FIPS, Common Criteria).
- ▶ Підтримувати середовища з різними пристроями, включно з твердотільними накопичувачами.
- ▶ Підтримувати диски з самошифруванням Trusted Computing Group (TCG) Opal v1.0.

Шифрування диска забезпечує захист окремих комп'ютерів та ноутбуків з системою Basic Input Output System (BIOS) та Unified Extensible Firmware Interface (UEFI).

Політики визначають, як працює програмне забезпечення шифрування диска на комп'ютері користувача. Процес шифрування диска є прозорим для користувача та майже не має впливу на продуктивність комп'ютера.

Функції шифрування диска забезпечують повне шифрування диска для ноутбуків та настільних ПК з ОС Microsoft Windows, а також запобігають витоку чутливих даних, особливо у разі втрати або крадіжки обладнання.

- ▶ **Централізоване управління** — Drive Encryption повністю інтегрується в Trellix ePO, використовуючи інфраструктуру Trellix ePO для автоматизованої звітності з безпеки, моніторингу, розгортання та адміністрування політик.
- ▶ **Прозоре шифрування** — шифрування без перешкод для користувачів або продуктивності системи.
- ▶ **Контроль доступу** — Drive Encryption забезпечує контроль доступу з попередньою аутентифікацією.
- ▶ **Відновлення** — дозволяє користувачу виконувати аварійне відновлення, коли систему не вдається перезавантажити або її файлова система перед завантаженням (PBFS) пошкоджена.
- ▶ **Підтримка дисків з самошифруванням** — Drive Encryption та Trellix ePO дозволяють централізоване управління самошифрованими дисками, які відповідають стандарту Opal від Trusted Computing Group (TCG), включно з блокуванням та розблокуванням, звітністю, відновленням, забезпеченням виконання політики та управлінням користувачами.
- ▶ **Trusted Platform Module (TPM)** — Шифрування диска підтримує TPM 2.0 на системах Windows 8 та пізніших версіях UEFI для забезпечення аутентифікації платформи без необхідності в попередній аутентифікації (PBA).

TRELLIX FILE AND REMOVABLE MEDIA PROTECTION (FRP)

Trellix FRP забезпечує автоматичне і прозоре шифрування файлів та папок, які зберігаються на ПК, файлових серверах, хмарних сховищах, електронній пошті та знімних носіях (USB-накопичувачі, CD / DVD та ISO-файли) або надсилаються на них. Trellix FRP переконується, що певні файли та папки завжди зашифровані, незалежно від того, де дані редагуються, копіюються або зберігаються. Ви можете створювати та забезпечувати централізовані політики на основі користувачів та груп користувачів для певних файлів та папок без участі користувача.

Trellix FRP дозволяє вам:



Отримувати доступ до зашифрованих даних в будь-якому місці без будь-якої додаткової установки програмного забезпечення або прав локального адміністратора на пристрої.



Шифрувати або блокувати записи на знімних носіях на робочих станціях VDI



Зберігати файли та папки у безпеці, де б вони не розташовувались, зокрема на локальних жорстких дисках, файлових серверах, знімних носіях та у хмарних сховищах (Box, Dropbox, Google Drive та Microsoft OneDrive).

Типові випадки використання Trellix FRP включають:

- ▶ Шифрування файлів, таких як електронні таблиці та конфіденційні документи
- ▶ Надання доступу до певної папки на спільній мережі
- ▶ Шифрування файлів, які синхронізуються з хмарними сховищами
- ▶ Шифрування знімних носіїв або блокування копіювання незашифрованих файлів
- ▶ Відправлення партнерам або клієнтам електронних листів з саморозпаковуваними файлами.

ОСНОВНІ ФУНКЦІЇ

Функції File and Removable Media Protection забезпечують шифрування даних на мережевих файлах та папках, знімних носіях, USB-портативних пристроях зберігання та у хмарних сховищах.

- ▶ **Централізоване управління** — забезпечує підтримку розгортання та управління Trellix FRP за допомогою програмного забезпечення Trellix ePO.
- ▶ **Особистий ключ користувача** — для кожного користувача може створюватись унікальний ключ шифрування.
- ▶ **Делеговане управління через управління ключами на основі ролей** — дозволяє логічно розділяти управління між кількома адміністраторами. Ця можливість є критичною для розділення функцій бізнесу та дочірніх підприємств.
- ▶ **Аудит управління ключами та призначення політик** — дії з управління ключами та призначення політик, які виконуються адміністраторами Trellix ePO, записуються в журнал аудиту. Ця функція є критичною для забезпечення відповідності та запобігання зловживанням з боку привілейованих адміністраторів.
- ▶ **Захист даних на знімних носіях** — дозволяє шифрування знімних носіїв та доступ до зашифрованого вмісту, навіть на системах, де Trellix FRP не встановлено.
- ▶ **Захист даних (включаючи аудит та звітність) для хмарних сховищ** — дозволяє шифрування синхронізованих папок на ПК для Dropbox, Box, Google Drive та OneDrive. Також забезпечує безпечний доступ до зашифрованих файлів на мобільних пристроях за допомогою додатка Trellix Endpoint Assistant.
- ▶ **Шифрування мережі** — дозволяє забезпечити безпечне спільне використання та співпрацю на мережевих ресурсах.
- ▶ **Ініціювання користувачем шифрування файлів та вкладень електронної пошти** — дозволяє користувачам створювати та додавати файли з паролем, які можна розшифрувати на системах, де Trellix FRP не встановлено.
- ▶ **Аудит та звітність подій зі знімних носіїв USB та CD / DVD / ISO** — записує всі дії користувачів, пов'язані з подіями зі знімними носіями USB та CD / DVD / ISO. Функція аудиту надає ефективний зворотний зв'язок для адміністраторів, які ухвалюють рішення про політику.
- ▶ **Використання загального криптографічного модуля Trellix (MCCM)** — Trellix FRP використовує модулі криптографії користувача та ядра FIPS 140-2 MCCM. Ви можете встановити Trellix FRP у режимі FIPS.

