KINGSTON IRONKEY™

Апаратне шифрування vs програмне шифрування

Розуміння основних відмінностей та вибір оптимального варіанту під власні потреби.

У безперервній боротьбі за безпеку даних різниця між апаратним і програмним шифруванням зводиться до того, де саме реалізовано засоби захисту та наскільки вони є вразливими в реальних умовах експлуатації. У випадку з USB-накопичувачами та SSD-накопичувачами те, де саме здійснюється шифрування, визначає ступінь захисту даних та ступінь їхньої залежності від навколишньої системи.

АПАРАТНЕ	VS	ПРОГРАМНЕ
Ключі шифрування Ключі шифрування генеруються внутрішньо апаратним забезпеченням і захищено зберігаються на накопичувачі.		**Ключі шифрування** Пароль користувача використовується безпосередньо як ключ шифрування, а ключі можуть зберігатися в системній пам'яті.
Захист від брутфорс-атак Ця функція призначена для захисту від брутфорс-атак шляхом обмеження кількості спроб, після чого накопичувач самостійно стирає дані, що унеможливлює доступ до конфіденційної інформації у разі його втрати або крадіжки.		**Захист від брутфорс-атак** Оскільки система вразлива до брутфорс-атак, комп'ютер намагається обмежити кількість спроб розшифрування, однак хакери можуть отримати доступ до пам'яті комп'ютера та скинути підрахунок спроб.
Вимоги до програмного забезпечення або драйверів На хост-системі не потрібно встановлювати драйвери чи програмне забезпечення.		**Вимоги до програмного забезпечення або драйверів** Необхідно встановити програмне забезпечення; вимоги до драйверів та сумісність з операційною системою можуть відрізнятися.
Засоби шифрування Використовує спеціальний криптографічний процесор, вбудований безпосередньо в сам накопичувач.		**Засоби шифрування** Використовує процесор та системні ресурси хост-комп'ютера для шифрування та дешифрування даних.
Залежність від хост-системи Система безпеки ізольована всередині пристрою і залишається захищеною навіть під час підключення до ненадійних або заражених комп'ютерів.		**Залежність від хост-системи** Система безпеки залежить від операційної системи хост-комп'ютера і є більш вразливою, якщо комп'ютер заражений шкідливим програмним забезпеченням.
Стан шифрування Шифрування є постійно активним за замовчуванням і не може бути вимкнене або обійдене.		**Стан шифрування** Шифрування можна увімкнути, вимкнути або неправильно налаштувати.
Вплив на продуктивність Вплив на продуктивність є мінімальним, оскільки шифрування виконується апаратним процесором.		**Вплив на продуктивність** Може негативно вплинути на продуктивність, оскільки шифрування використовує ресурси процесора.
Гнучкість Шифрування прив'язане до конкретного USB-накопичувача або SSD-диска.		**Гнучкість** Може бути реалізовано практично на будь-якому носії.

Програмне шифрування забезпечує гнучкість, в той час як апаратне шифрування ізолює систему безпеки та зменшує її вразливість до ризиків на системному рівні. Розуміння того, як кожна з цих технологій захищає дані та контролює доступ, допоможе вам обрати оптимальний рівень безпеки, що відповідає вашим робочим процесам та профілю ризиків.

www.kingston.com/ironkey