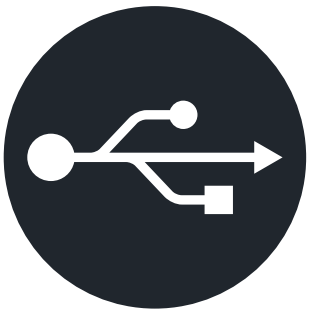
Як надати доступ до USB-накопичувачів

без погіршення рівня безпеки кінцевих точок

#KingstonIsWithYou #KingstonIronkey

Вступ

У січні 1996 року вихід офіційної специфікації USB 1.0 символізував собою нову епоху однотипності, зручності та універсальності як для постачальників периферійних пристроїв, так і для кінцевих користувачів. 27 років по тому USB забезпечує зворотну сумісність із всіма попередніми версіями та залишається найважливішим елементом інтерфейсу комп'ютерного обладнання — від серверів до смартфонів.



Завдяки простоті технології «plug-and-play» та постійному підвищенню швидкості, портативні USB-накопичувачі зайняли одну з провідних позицій на ринку. Але за цю зручність доводиться платити зниженням рівня безпеки даних. У сучасному світі, не маючи відповідних засобів захисту кінцевих точок на комп'ютерах і належних практик захисту інформації, користувачі, які недбало ставляться до використання портативних USB-накопичувачів, наражають себе та інших людей на небезпеку витоку даних. Це може коштувати кінцевому користувачеві занадто дорого або навіть поставити під загрозу безпеку усієї організації чи уряду.

Окрім захисту хост-середовища, USB-накопичувач також має бути захищений паролем і апаратним шифруванням на пристрої. Це дає змогу максимально захиститися від будь-яких спроб втручання. Ми обговоримо деякі передові практики безпечнішого використання USB-накопичувачів, а також докладніше розглянемо USB-пристрої.

Ідеальним рішенням вважається комбінований підхід, проте первинне значення мають надійність шифрування та апаратні компоненти самого USB-накопичувача. Ці накопичувачі здатні принести користь таким секторам, як фінанси, медицина, виробництво та військова справа. Вони також застосовуються під час дистанційної роботи, коли доступ до мережі або недоступний, або вразливий, або недоцільний.

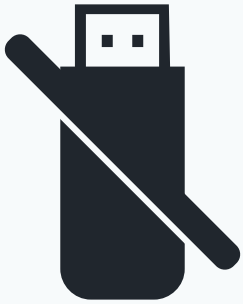
USB-накопичувачі з апаратним шифруванням мають різні класи захисту та ряд функцій безпеки. Завдяки своїм характеристикам і можливостям кастомізації ці накопичувачі також можуть використовуватись як автономні рішення в будь-якому чутливому середовищі.

Поводження з портами: USB-накопичувачі взаємодіють з програмним забезпеченням з адміністрування кінцевих точок задля запобігання втраті даних

Упродовж десятиліть застосунки для захисту від вірусів і шкідливих програм гарантували захист на найвищому рівні, автоматично скануючи завантажені файли або підключені пристрої та повідомляючи про підозрілий вміст або реагуючи на нього відповідно. Захист, що забезпечується антивірусним програмним забезпеченням нового покоління (NGAV), робить ще один крок у цьому напрямку. Замість того, щоб покладатися виключно на базу вірусних сигнатур, що постійно оновлюється, NGAV додає функції машинного навчання та виявлення на основі поведінки, які можуть розпізнавати та усувати ще невідомі їм загрози.

Проте це не єдина зброя в арсеналі, тому якщо вам потрібний куленепробивний захист даних на користувацьких периферійних пристроях, програмне забезпечення з адміністрування кінцевих точок задля запобігання втраті даних (Data Loss Prevention, DLP) дає змогу обмежити будь-який доступ до USB-портів та інших точок доступу.

Підхід до безпеки за принципом «блокувати всі порти», безумовно, може усунути ризики та стати доречним за певних обставин, але така політика зазвичай виявляється дуже неефективною й призводить до небажаних наслідків.



Деякі IT-адміністратори вважають за потрібне відхиляти запити на розблокування USB-портів на комп'ютерах користувачів, оскільки це відкриватиме прямий доступ через корпоративний брандмауер. Така обережність цілком зрозуміла, але коли справа доходить до надання доступу до USB-накопичувача, надання такого привілею не має створювати серйозну загрозу безпеці за умови дотримання певних вимог.

Важливою вимогою є пакет програм з адміністрування кінцевих точок, який містить систему сканування та виявлення загроз у застосунках для захисту від вірусів і шкідливих програм, а також централізований моніторинг і адміністрування всіх кінцевих точок користувачів.

Зазвичай цей прямолінійний підхід реалізується різними способами в уніфікованих рішеннях від популярних постачальників, як-от McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection і WinMagic SecureDoc.

Удосконалення — налаштування білих списків

Якщо ми говоримо про захист USB-накопичувачів, відповідний метод залежить від необхідного рівня захисту. Простий, але ефективний підхід — додати USB-накопичувачі в білий список, використовуючи їх ідентифікатор постачальника (VID) та ідентифікатор продукту (PID). Усі периферійні USB-пристрої мають одну особливість: у будь-якого виробника є свій унікальний ідентифікатор VID, але ідентифікатор PID змінюється для кожного нового продукту.

Використання виключно VID виробника призведе до значного розширення білого списку та погіршення рівня безпеки, оскільки дозвіл отримуватимуть усі USB-пристрої, виготовлені цим виробником. PID є більш вдосконаленим ідентифікатором, який вимагає надання доступу до головного комп'ютера лише певній моделі.

Це вже набагато краще, але ще не ідеально. USB-накопичувачі користуються величезним попитом, і користувачі можуть придбати собі пристрій, який не відрізняється від пристрою, до якого було надано доступ. Розуміючи це, Kingston Technology пропонує індивідуальне рішення для посилення безпеки USB-накопичувачів.

За допомогою програми кастомізації можна створити унікальні профілі PID для конкретної організації та запровадити їх до лінійки USB-накопичувачів із шифруванням від Kingston. Компанії, які розгортають пристрої зі спеціалізованим ідентифікатором продукту, не лише виграють від оптимізації білих списків, але й значно підвищують рівень безпеки. Без відповідного унікального PID будь-які пристрої, придбані співробітниками самостійно, навіть якщо вони здаються ідентичними, будуть позбавлені доступу.

Хоча використання унікальних ідентифікаторів PID допомагає IT-адміністраторам швидко й легко вводити в експлуатацію нові USB-накопичувачі, більш гнучкою альтернативою є використання індивідуальних серійних номерів

пристроїв, які присутні на більшості USB-накопичувачів із шифруванням від Kingston. Кожен унікальний серійний номер пристрою має бути зареєстрований у пакеті адміністрування кінцевих точок. Спочатку ця робота передбачає задіяння IT-персоналу, і компанія Kingston може надати список серійних номерів для кожного замовлення (вони завжди складаються із літер та цифр і ніколи не бувають послідовними). Вибір цього способу дає змогу застосовувати набагато гнучкіші політики на підставі власності кожного окремого накопичувача, а також забезпечує додаткову перевагу — високоточне відслідковування походження пристроїв, що може виявитися безцінним у сценаріях криміналістичної IT-експертизи. Деякі накопичувачі Kingston містять серійний номер і штрихкод на корпусі для електронного сканування, а решту пристроїв можна налаштувати, додавши на корпуси відповідний штрихкод і серійний номер; ці елементи можна використовувати для відслідковування накопичувачів.

За замовчуванням системи адміністрування кінцевих точок надають доступ до ідентифікаторів VID/PID для блокування портів і внесення в білий список. Компанія Kingston пропонує ефективніший спосіб використання цих функцій, створюючи більш гнучкі та витончені політики, які полегшують використання USB-накопичувачів. Якщо запровадити відповідний спосіб ідентифікації, загальна позиція «блокувати всі порти» не лише істотно спрощується, але й стає непотрібною.

Безпечні рішення для віддалених користувачів, що відповідають нормативним вимогам

Коли йдеться про безпеку, ведення білих списків пристроїв — це лише половина проблеми, або, інакше кажучи, половина рішення.

Зручність і простота USB-накопичувачів робить їх незамінними у багатьох компаніях і установах, які розглядають портативність як ключовий елемент забезпечення безперебійної передачі даних. У більшості компаній, з міркувань дотримання нормативних вимог і вимог IT-гігієни, необхідно оснастити персонал USB-накопичувачами з шифруванням для виконання подібних операцій. Завдяки парольному захисту та шифруванню портативний накопичувач унеможливлює доступ до конфіденційних даних після втрати, крадіжки або залишення цього пристрою в потенційно вразливій ситуації.

Універсального рішення не існує, оскільки використовуються різні методи шифрування, а найбільш помітні відмінності починають виявлятися після порівняння програмних і апаратних засобів для шифрування. Отже, яке з рішень найкраще? Усе залежить від ваших потреб, але важливіше поставити запитання: «Яке з рішень безпечніше?»

Програмне шифрування — це, по суті, бюджетний варіант, який задовольнить вимоги деяких дрібних підприємств. Також це рішення підходить компаніям, які не вважають конфіденційною інформацію, що передається, і для яких головною проблемою залишається дотримання положень політик.

Проте сам принцип дії програмного шифрування виявляється його найбільш вразливим місцем, оскільки для процесу шифрування потрібні застосунки з боку клієнта, залежні від його комп'ютера. Відповідно, накопичувач із програмним шифруванням захищений настільки, наскільки захищений комп'ютер, до якого цей накопичувач підключений.

Уразливість системи також зростає, оскільки хакери, отримавши доступ до пам'яті комп'ютера, можуть розкрити ключі шифрування/розшифрування. Дані на накопичувачі також можуть зазнати атак методом перебору паролів, і захист паролю від перебору не допоможе, якщо зашифровані файли можна скопіювати.

Не забувайте, що програмне шифрування, ймовірно, вимагатиме регулярного оновлення програмного забезпечення, що може ускладнити процес розгортання, створивши додаткове навантаження на IT-персонал. І найгірше тут те, що програмне шифрування може бути повністю видалене розчарованими співробітниками, які зіткнуться з проблемами з переносимістю накопичувача між різними платформами. Користувачі накопичувачів можуть скопіювати зашифровані дані з накопичувача на комп'ютер, переформатувати накопичувач, зробивши його нешифрованим, а потім знову скопіювати дані на нього уже без шифрування. З цього моменту ваші дані стануть незахищеними та повністю вразливими для атак. Це неприпустимо, якщо ви дотримуєтесь законів і норм щодо захисту даних, оскільки програмний захист USB-накопичувача може бути повністю деактивований.

Шифрування на чипі: надійне та швидке рішення

На противагу програмному шифруванню, USB-накопичувач з апаратним шифруванням функціонує незалежно від комп'ютера, оскільки він оснащений вбудованим у фізичний пристрій окремим процесором для шифрування. В такому накопичувачі процес шифрування неможливо вимкнути, та він захищений від атак методом перебору паролів. Зашифровані дані на такому накопичувачі недоступні й не можуть бути скопійовані.

В USB-накопичувачах Kingston із апаратним шифруванням корпоративного та військового рівнів застосовується шифрування AES 256-bit у режимі XTS. Технологія шифрування AES 256-bit схвалена у всьому світі і максимально захищає дані на пристрої. Завдяки використанню двох окремих ключів на різних етапах процесу шифрування/розшифрування, режим XTS діє подібно подвійному шифруванню даних.

Ключ шифрування створюється генератором випадкових чисел у контролері накопичувача, який розблоковується паролем користувача. Оскільки автентифікація відбувається всередині криптомодуля, ключі шифрування та інші критично важливі функції безпеки залишаються захищеними від найпоширеніших типів атак, як-от BadUSB, атаки холодного перезапуску, атаки шкідливого програмного забезпечення або атаки методом перебору паролів.

Однією з миттєвих переваг апаратного шифрування є істотне підвищення продуктивності, порівнюючи з програмним шифруванням, оскільки більше не потрібно переносити сам процес шифрування на комп'ютер, до якого підключений накопичувач. Увесь процес відбувається всередині накопичувача.

USB-накопичувачі з апаратним шифруванням, як-от Kingston IronKey D500S, — це захищені паролем пристрої, які шифрують дані завжди. Спочатку користувач бачить лише захищений від запису розділ, який містить застосунок для автентифікації пароля та розблокування основного зашифрованого тому накопичувача. Ця процедура запобігає встановленню будь-яких драйверів або програм на комп'ютер.

Крім того, USB-накопичувачі з апаратним шифруванням від Kingston оснащені прошивкfами з цифровим підписом, які запобігають будь-яким маніпуляціям із прошивкою пристрою. Цей додатковий рівень безпеки захищає накопичувач від атак BadUSB, які використовують внутрішню вразливість прошивки USB-пристрою. Подібна атака може призвести до прихованого виконання команд або запуску шкідливого коду на комп'ютері.

Звісно підхід за принципом «блокувати всі порти» може обмежити кількість атак типу BadUSB, але навіщо жертвувати продуктивністю, використовуючи такі застарілі практики? Як вже зазначалося вище, можна підтримувати належний рівень безпеки одночасно з використанням портативних накопичувачів, запровадивши зрозумілі процедури закупівлі та введення в експлуатацію USB-накопичувачів з апаратним шифруванням.

Безпечна дистанційна робота, що відповідає нормативним вимогам

Для віддалених співробітників, які перебувають за межами безпечного робочого середовища організації, потрібно оновити стратегію, а також переглянути пріоритети.

Коли ми говоримо про планування безпеки дистанційної роботи, чи є якась користь у блокуванні портів USB на ноутбуку вашого співробітника, якщо він приєднується через Інтернет до сервера, щоб передати або завантажити документи? Коли співробітник перебуває в дорозі, єдиним доступним засобом може виявитися відкрите інтернет-з'єднання, як-от незахищена або ненадійна точка доступу Wi-Fi, що створює безліч загроз безпеці, які істотно збільшують ймовірність злому. Такі загрози, як перехоплення даних і спостереження з використанням

спуфінгу, атаки типу «людина посередині» (MitM) і прослуховування в мережі — це лише деякі з найвитонченіших методів злому, які доступні кіберзлочинцям. Навіть VPN зазнають ризику.

Мережеве підключення організації до Інтернету — це ще одна кінцева точка, тому її незахищеність робить її надзвичайно вразливою та головною ціллю для атаки. Відкриття віддаленого доступу пов'язане з певними ризиками, особливо коли йдеться про конфіденційні дані.

Оснащення віддалених співробітників захищеними паролем USB-накопичувачами з апаратним шифруванням ефективно усуває потенційні вразливості в мережі. Але для цього потрібно ретельніше вивчити доступні USB-накопичувачі та їх відповідність вимогам кожного віддаленого робочого середовища. Йдеться не про вибір ємності накопичувача чи реєстрацію серійного номера пристрою, а про фізичну конструкцію самого пристрою.

Засоби захисту від злому: надійні варіанти

Головне питання полягає в тому, чи захищений USB-накопичувач з апаратним шифруванням від злому. Ступінь захищеності пристрою від подібного втручання відображена в такому стандарті, як FIPS 140-3. Він має кілька рівнів, які досліджують стійкість фізичної конструкції накопичувача без використання криптографічних методів.

Відповідна сертифікація за стандартом FIPS-197 поширюється тільки на атрибути апаратного шифрування та стосується таких пристроїв, як зовнішні SSD-накопичувачі серії IronKey Vault Privacy 50 та Vault Privacy 80, які орієнтовані на підприємства й не відповідають вимогам армійських стандартів до безпеки даних. Ці накопичувачі дешевші, але не захищені від фізичного злому.

Сертифікація за стандартом FIPS 140-3 Level 3 (наразі очікується) означає, що методи, які використовуються для виявлення злому, відповідають армійським стандартам. Компанія Kingston пропонує накопичувачі, що відповідають стандарту FIPS 140-3 Level 3, підприємствам, урядам і збройним силам у всьому світі.

Для захисту накопичувача використовується епоксидна смола, що покриває внутрішні мікросхеми пристрою, а приклеювання внутрішніх компонентів до корпусу створює ще одну «стіну захисту». Будь-яка спроба розкрити металевий корпус буде вкрай ускладнена й призведе до фізичного руйнування внутрішніх мікросхем та інших компонентів, і накопичувач стане непрацездатним. За наявності непрозорої епоксидної смоли, яка полімеризується до твердого стану, втручання в критично важливі компоненти стає практично неможливим. Цей додатковий засіб захисту використовується в таких пристроях, як Kingston IronKey D500S і S1000.

Безпека пристроїв не обмежується лише фізичними засобами захисту. Накопичувач Kingston IronKey S1000 виводить захист від злому на абсолютно новий рівень. Вбудований в IronKey S1000 крипточип може виявити будь-яке фізичне втручання та зробити накопичувач непридатним для використання після ввімкнення пристрою. Використання USB-накопичувачів з апаратним шифруванням для отримання доступу до конфіденційних файлів та їх передачі — це практичний крок, який спрощує дистанційну роботу та гарантує безпеку в польових умовах.

Обов'язково перегляньте апаратні особливості та функції безпеки USB-накопичувачів, щоб дізнатися, чи відповідають вони вашим потребам і сценарію використання. Кожну модель USB-накопичувача необхідно перевіряти окремо, звертаючи увагу на сертифікації, що допомагають визначитись у вашому виборі. Якими б не були ваші пріоритети, компанія Kingston пропонує широкий спектр USB-накопичувачів з апаратним шифруванням і варіантів їх налаштування за доступними цінами. Вони призначені для різних середовищ і відповідають як загальним нормативним вимогам, так і найжорсткішим армійським специфікаціям.

Безпека передусім: немає мереж, немає проблем

У сучасному світі офіс немає меж, і, оскільки робота з дому продовжує бурхливо розвиватися, багато компаній починають звертати увагу на проблеми вразливості дистанційного доступу. Багато хто стикається з подібними проблемами вперше та шукає безпечніші способи адаптуватися до нових реалій.

Для задоволення цих потреб у широкому спектрі галузей використовуються USB-накопичувачі з апаратним шифруванням, які дуже добре зарекомендували себе та пропонують надійний захист у ситуаціях, коли передача даних через мережу може бути недоцільною або небажаною з ряду причин.

У сфері фінансів регуляторні органи часто запитують дані для перевірки діяльності компанії та дотримання нею нормативних вимог. Ризик витоку даних занадто великий, щоб розглядати можливість використання мережі для передачі конфіденційних документів, що містять точні дані про інвестиції, торгівлю на ринках та іншу чутливу інформацію про банківську діяльність. Простим і ефективним рішенням є передача цієї інформації за допомогою USB-накопичувача з апаратним шифруванням.

Використання захищених USB-накопичувачів для передачі файлів у медичних установах — повсякденне явище. Це також обумовлено зручністю для лікарів або медичних консультантів, які можуть захотіти проаналізувати файли, звернутися до них під час дослідження або надати приклади з практики студентам-медикам. Існують і більш практичні потреби, коли йдеться про патентовані системи, наприклад, пристрої діагностичної візуалізації з відсутнім або незахищеним доступом до мережі. Сумісні USB-накопичувачі з апаратним шифруванням можуть легко переносити файли для використання в інших місцях.

Що можна і що не треба робити

✓ **Використовуйте сумісні та захищені накопичувачі,** а також перегляньте специфікації, щоб придбати накопичувачі, які відповідають потребам кожного сценарію розгортання.

✗ **Не допускайте використання випадкових накопичувачів або практики «принесіть свій власний пристрій» (BYOD)** — для будь-якої компанії втрата незашифрованих накопичувачів пов'язана із занадто високим ризиком фінансового та репутаційного збитку.

✓ **Розгорніть пакет адміністрування кінцевих точок** та використовуйте USB-накопичувачі з апаратним шифруванням, оснащені спеціальними можливостями підтримки білих списків.

✗ **Не покладайтеся на випадок.** Правильно оцініть вимоги до локального та віддаленого робочого середовища.

✓ **Проведіть для співробітників інструктаж** з питань безпеки. Це в їх інтересах, щоби компанія залишалась захищеною від загроз інформаційній безпеці.

✗ **Не створюйте обтяжливих незручностей для користувачів,** оскільки вони почнуть шукати обхідні шляхи, що призведе до використання тіньових IT-рішень. Той факт, що політика тотального контролю застосовувалася завжди, не означає, що вона підходить для всіх сценаріїв. Робоче середовище змінюється, і, вибираючи відповідні рішення, є можливість розробляти та впроваджувати нові політики.

Тут на перший план виходить накопичувач Kingston IronKey Keypad 200 (KP200). У цьому незалежному від операційних систем накопичувачі відсутній том програми запуску для введення пароля. Натомість використовується літерно-цифрова клавіатура, яка розблоковує пристрій для використання на будь-якій платформі. Подібно до швейцарського армійського ножа, використання USB-накопичувачів з апаратним шифруванням поширюється й на виробничу діяльність. Вони служать для перенесення програм, створених у сфері дослідження та розробки інформаційних технологій, на обладнання, що контролюється платформами операційних технологій (OT). KP200 — одне з найпростіших і захищених рішень для роботи зі змішаними платформами, в яких також використовується ОС Linux.

Правоохоронні органі також покладають великі сподівання на USB-накопичувачі з апаратним шифруванням. Вони захищають і надійно передають матеріали справ, фотографії та інші докази оперативникам на місцях, слідчим органам і судово-медичним експертам. Компанія Kingston пропонує додаткові переваги, постачаючи накопичувачі з вбудованим серійним номером, надрукованим на зовнішньому корпусі разом із штрихкодом. Випуск і каталогізація накопичувачів спрощуються та легко відслідковуються. Це так само просто й швидко, як вручну зареєструвати серійний номер або відсканувати штрихкод — проводити аудит і управління матеріальними запасами стало ще простіше. Ця функціональність є стандартною для накопичувачів Kingston IronKey D500S, D500SM і S1000B/E, але вона також доступна для інших моделей із апаратним шифруванням у рамках програми кастомізації Kingston.

Безпека та мобільність накопичувачів: останні досягнення

Захист паролем, апаратне шифрування, засоби захисту від злому, гнучкий білий список кінцевих точок, сертифікація за стандартом FIPS 140-3 Level 3 (очікується) та оперативне ведення журналу — це стандартні функції USB-накопичувачів компанії Kingston, які можна запровадити без жодних зволікань.

Ці надійні механізми безпеки гарантують, що USB-накопичувач і розміщені на ньому дані залишатимуться захищеними у хост-середовищі. Незважаючи на вражаючі заявлені технічні характеристики, вибір моделі навмання без жодних досліджень не обов'язково гарантуватиме відповідність пристрою жорстким вимогам деяких організацій.

Як незалежний виробник, компанія Kingston пропонує широкий спектр рішень для задоволення потреб клієнтів. У рамках програми кастомізації Kingston доступні сучасні рішення, спрямовані на покращення користувацького досвіду.

Налаштування безпеки не обмежується наданням організації власного ідентифікатора PID для внесення у білий список. Профіль безпеки програми запуску також можна конфігурувати, використовуючи п'ятнадцять різних налаштувань: від контактних даних і відомостей про компанію до ввімкнення підказок для пароля та визначення максимальної кількості спроб введення пароля. На зовнішньому корпусі може бути розміщений фірмовий знак (логотип) компанії. Крім того, для деяких моделей накопичувачів доступні різні кольори. Замовивши щонайменше п'ятдесят накопичувачів, ви отримуєте всі ці функції, призначені для швидкого введення пристроїв в експлуатацію.

Якщо програма для адміністрування кінцевих точок поки відсутня, то для організацій, які бажають адмініструвати свій парк накопичувачів Kingston, доступне відповідне рішення з можливостями віддаленого скидання паролів.

Завдяки своїй розповсюдженості та зручності технологія USB пережила безліч інших перспективних технологій, а для виконання багатьох операцій незмінними чинниками залишаються швидкість і зручність USB-накопичувачів. Легкодоступні та завжди захищені USB-накопичувачі — це прості рішення, яке можна оцінити вже зараз.

Навіщо турбуватися про витоки мережевих даних у віддалених середовищах? Завдяки USB-накопичувачу з апаратним шифруванням компанії Kingston відповідь на це запитання знаходиться буквально у вас на долоні.

Щоб дізнатися більше про рішення, які пропонує компанія Kingston, відвідайте вебсайт kingston.com/ironkey. Щоб отримати відповіді на більш конкретні запитання, зверніться до наших фахівців у сфері розробки USB-накопичувачів із шифруванням.

#KingstonIsWithYou #KingstonIronkey