
# SOFTWARE ENCRYPTION AND REGULATORY COMPLIANCE: LESS EXPENSIVE SOLUTION WITH MAJOR SECURITY RISKS

## REGULATORY AND COMPLIANCE REQUIREMENTS

Data security used to be relegated to IT departments only. However, due to continuous consumer data breaches, governments worldwide have imposed ever-increasing requirements on businesses to encrypt and protect all data that is personally identifiable.

From HIPAA in healthcare, to GDPR in EMEA and CCPA in California, encryption of protected data classes is being mandated through regulations. Compliance organisations have multiplied exponentially over the last 3+ years as these regulations and their associated fines and legal award risks have skyrocketed.

With these changes, IT departments have struggled to keep up with security and rising costs. Throughout the COVID pandemic, budgets are being spent on additional hardware and firewall investments, at the expense of a focus on data encryption.

In fact, software encryption using Microsoft BitLocker® or endpoint management software from companies like Symantec, McAfee and others is on the rise. Some businesses and consumers also use standard USB drives with software "vault" drives as provided by some vendors.

## ENCRYPTION AND DATA IN TRANSIT

Employees and consumers have a need to take their data with them. They have options such as using:

1. Cloud services: These are great, as they can be accessed from any device that can connect to the internet. However, flexibility comes at a price. Data storage on clouds removes control of the data from the user or the company and poses a potential risk, as we have seen cloud servers being left unlocked or accessed by unauthorised parties.
2. Standard USB drives: While carrying a USB drive seems more secure, the risk of data exposure through the loss of the drive can be significant. For example, stories abound of lost USB drives being found with secret information or of laundries with drawers full of lost USB drives.
3. Hardware-encrypted USB drives: These USB drives have custom architectures which incorporate an onboard encryption controller and access control. The data is generally encrypted using the strongest AES-256 bit encryption in XTS mode, along with other possible safeguards to mitigate physical and firmware based attacks. These drives are manufactured by companies that specialise in security devices, and while more expensive than standard USB drives, offer better data security. FIPS 197 or FIPS 140-2 Level 3 drives can add greater levels of protection and peace of mind.
4. Standard USB drives with software encryption: To provide security in line with regulations, software encryption with BitLocker or other tools can be used – they are decent options as they are relatively inexpensive and offer the same AES-256 XTS encryption.

It's no surprise to find out that, in most cases, businesses and industries tend to go with option 4, using Standard USB drives with software encryption, mainly because software encryption such as BitLocker or other data vault utilities are "free".

## SOFTWARE ENCRYPTION IS NOT COMPLIANT WITH REGULATIONS


For a business security professional, software encryption can offer the exact same encryption capabilities as more expensive hardware-encrypted USB drives. But is it the way to go? Budgets are strained, so businesses are moving to software encryption for compliance purposes, unaware of the dark side of software-based encryption.

What's the issue with software-encrypted USB drives? Is the data at rest and in transit not encrypted at AES-256 XTS? In general, it is. The problem is that software encryption is considered to be "removable encryption".

Wait – removable? Does that mean that a software-encrypted USB drive can have its encryption disabled by a user?

The answer is "Yes". Users can remove the software encryption feature from their USB drives. Why would they, you ask? Because they can – and because they just want to access the files without using a password or they simply forgot the password but need to use the USB drive.

## HOW TO REMOVE SOFTWARE ENCRYPTION FROM AN ENCRYPTED USB DRIVE

For a user who does not want to deal with entering complex passwords or other passwords to access their data, the process is simple:

1. Plug the software-encrypted drive into a computer
2. Format the drive
3. After the drive is formatted, all encryption is removed
4. Copy files with secret or confidential information to the drive for easy access

This is easy for users to do using a computer that is not restricted – IT departments have restricted the use of formatting commands on company computers, but this procedure can be performed on any other non-company computer.

For compliance purposes, the ease of removing data encryption means that the company-provided drive is now unencrypted, although the data that was encrypted on the drive is considered lost forever once the encryption is removed via the method above (encryption keys are tied to data). Any data copied onto the device once the encryption is removed is considered unsecured and potentially out of compliance, which can risk a violation of regulations such as HIPAA, GDPR, CCPA and many others.

## THE CONSEQUENCES OF UNENCRYPTED DRIVE LOSSES

If a company-designated USB drive is lost and found, even if the company is unaware at first but learns about it later through social media, special compliance requirements kick in for the company, which may require it to:

1. Conduct a forensic investigation to identify what data was lost
2. Determine if a legal breach has occurred, in consultation with the Legal department
3. Determine if customers must be notified

This is where a single USB drive loss can become very expensive. With legal costs in excess of many hundreds of pounds an hour, this compliance process can result in thousands and thousands of pounds in expenses, in addition to potential fines, customer and other lawsuits, and embarrassment from data exposure.

When software encryption is considered for its low-cost implementation, these risks and their huge financial consequences are not taken into account.

There is another danger to allowing the use of unencrypted USB drives on a company network. It is commonly called "BadUSB". BadUSB is a class of malware that has been used by bad actors to breach a company's firewall and introduce malware into a company's cyber-defences through USB storage devices.

## BadUSB


When a USB drive is plugged into a computer, the chipset controller of the computer starts a handshake with the USB drive controller via firmware. This exchange occurs before the operating system, such as Microsoft/MacOS/Linux, is even aware that a USB drive has been connected. Every USB drive has firmware that runs when the drive is plugged into a USB port.

Bad actors have learned that they can introduce malware through this handshake mechanism by replacing the firmware that runs on the USB drive by another, more malicious firmware that injects malware into the target computer system as it communicates with the USB drive. A standard USB drive has no security on its internal firmware that is executed by its controller, so BadUSB was born as good USB drives were weaponised to penetrate firewalls and breach cyber defences.

Many companies try to ban the use of USB drives on their systems, or even go as far as to fill USB ports with epoxy. However, they found that classes of employees need to carry data with them on USB drives. For example, executives want to take data with them to work on or provide to external legal or financial advisors who are not on a company cloud; company contractors need data to work on but with restricted access to company databases; financial analysts who are rushing to close the monthly reports need to work on spreadsheets at home.

As the previous analysis shows, there is a significant risk to using this standard USB drive plus software encryption solution. At first glance, what appeared to be cheaper turns out to be potentially very harmful and much more expensive. Just the cost of 2-3 hours' consulting with a lawyer about a potential data breach wipes away any savings from using the cheaper solution.

## HARDWARE-ENCRYPTED USB DRIVES ARE THE BEST OPTION FOR REGULATORY COMPLIANCE

What makes hardware-encrypted USB drives the best choice for these regulatory applications:

1. Hardware-encrypted USB drives have encryption that is always ON: There is no way for users to turn off encryption, reset the password rules (minimum length, complexity) and disable the automatic password retries. Unlike software encryption, which does not prevent repeated password guessing through software dictionary attacks, the hardware versions limit password retries – and lock down the data when the wrong passwords are entered 10 times or sometimes even fewer. This is very secure in the age of supercomputers.
2. Hardware-encrypted drives use premium encryption controllers and incorporate many security features: While we don't always disclose all security countermeasures, there is a countermeasure to protect against BadUSB. At the factory, when the firmware is loaded on hardware-encrypted drives only, the firmware is digitally signed and loaded. This means that, when these encrypted USBs are plugged in, the encryption controller first checks the integrity of the firmware through the digital signature, and only loads it if it passes the verification. Any attempt to replace the firmware will brick the drive and it will become non-functional – and no threat.
3. Hardware-encrypted USB drives can have custom Product IDs (PIDs) set up for a specific company: These premium drives can have a digital identifier programmed into them so that if a drive is plugged into the company's inner or outer firewall, the drive can be identified as a company-issued drive. For example, if an employee loses the company drive and buys the same model at retail, the newly purchased drive will not validate on the company network. This customisation adds another layer of security to the use of USB drives.
4. Hardware-encrypted drives save money very quickly: Just the reduction and elimination of risks makes the payback cycle very short.

Kingston is the world's largest manufacturer of encrypted USB drives and offers drive families with various features and price points. Contact Kingston directly to discuss how we can help you stay compliant with encrypted USB solutions for executives, employees, contractors and more.