

## 6 Reasons Why Software-Based Encryption Doesn't Stack Up

As organizations everywhere move to secure their critical data and assets while trying to comply with industry regulations, the choice to provide workers with encrypted USB devices is often an obvious one. One important consideration in choosing a portable security device is the choice between hardware-based and software-based encryption. This paper examines the key differences between these two methods of encryption used by USB device providers.

### Encryption of USB Drives

Your employees carry USB drives, and you're already informed enough to know that you want the data they hold encrypted – after all, it's the same information you strongly protect while it's on your network, but with the added problem of being easily lost or stolen.

Your next challenge is to understand the difference between software and hardware encryption, so you can be sure you're getting what you need. Your requirements likely include:

- Mandatory Encryption. Is all data actually encrypted?
- Resistance to Attack. How safe is the data?
- Deployability. What's the impact on my IT staff?
- Usability. What's the impact on my users?

This discussion paper will compare software and hardware encryption for each of these categories.

### Defining Software and Hardware Encryption

Software encryption takes the data to be protected and encrypts it on the user's computer. Security software runs on the computer, takes in the data and a secret key, and performs the encryption operation using the key. To protect this secret key, software encryption products actually encrypt it with a user password. All of this is written to one or more files on the USB drive.

To get access to the protected data with software encryption, the user enters their password, which decrypts the secret key. The key is then used to decrypt the protected data itself.

Hardware encryption takes the data to be protected and encrypts it within an actual hardware device, separate from the user's computer. The device uses an internal secret key and encrypts the data. The secret key never leaves the device.

To get access to the protected data with hardware encryption, the device is unlocked by the user with a password, fingerprint scan, or other form of identity verification. The device itself validates these credentials, and makes the secure data available, decrypting it as it's read off the device.

# Hardware-Based Versus Software-Based Encryption

## Mandatory Encryption

Most software encryption products that support USB devices do not and cannot make encryption mandatory. If they wish, users can bypass the security features and simply copy data to the USB drive unencrypted. This user behaviour can be quite common, especially as most software encryption products require extra steps and proprietary user interfaces to encrypt data.

Hardware encryption products require that users must unlock the USB drive in order to use it. All data placed on the device after this point is automatically encrypted, enforcing security.

## Resistance to Attack

Encryption is chosen to prevent an interested party from reading sensitive information. The question is, how effective is the encryption process itself?

Most good software and hardware encryption products will support the Advanced Encryption Standard (AES) encryption algorithm, and the better ones will employ AES-256, meaning that a 256-bit secret key is used. But even if two products use AES-256, there are several security differences if one product uses software encryption and the other hardware encryption.

## Security of the Password

Software encryption products typically store the secret key in a file on the USB drive, and encrypt it with the user's password. If an attacker can get to the drive, they can get a copy of this file. With a computer or two, an attacker with minimal technical knowledge can use a password cracking program to guess the password – even passwords 15 or more characters long – in a matter of days, exposing the data.

With hardware encryption, validation of the password is done inside the USB drive itself. Devices usually introduce time delays upon getting a bad password, meaning the time to crack a password increases dramatically. Some devices will even go into a lockdown mode or possibly erase all on-board after getting a certain number of bad passwords, eliminating the threat of this attack altogether.

## Security of the Secret Key

Since software encryption needs the secret key on the computer, it tends to get written to the operating system's virtual memory swap file, where it can persist for hours or days after the device leaves. After finding the key in this file, a difficult but doable task, an attacker can gain access any encrypted data on the device as easily as if it were not encrypted at all.

Hardware encryption never allows the secret key to leave the USB drive, preventing such attacks.

# Hardware-Based Versus Software-Based Encryption

## Hidden Unencrypted Data

The flash memory in a USB drive uses a process known as wear leveling that increases the longevity of memory cells by not reusing the same memory location too often, and not actually erasing any data until it's overwritten by new data.

The non-mandatory nature of software encryption makes this memory behaviour a real problem. If a user writes unencrypted data to the drive, it can remain on the drive for a very long time, where it is recoverable by an attacker. Deleting a file, overwriting a file with an encrypted version, and similar operations simply don't guarantee that the unencrypted data gets removed.

Since hardware encryption is always on, this aspect of flash memory behaviour poses no security risk – any left-over data is known to be encrypted and safe.

## Malware

Since software encryption runs on the user's computer, it is open to attack by viruses and other malware (including targeted malware), putting data and its integrity at risk. Hardware encryption takes place within the USB drive itself, isolating it from any malware on the user's computer.

\*Malware written specifically to attack the software encryption product.

## Deployability

### Installation

Software encryption is just that – a piece of software. This software must be installed on every system where a user wishes to use their USB drive. Such software typically includes device drivers that handle encryption/decryption, meaning administrative privileges are required for installation.

Hardware encryption requires no software installation or administrative rights on the target system, allowing the USB drive to be used on any computer quickly and easily.

### Up-Front Cost

Software encryption typically works with any off-the-shelf USB drive. Costs are similar to the cost of other client-side security applications, and are usually priced per user.

Hardware encryption, as part of the USB drive, requires purchase of specific USB drives. Purchase cost is usually similar to software encryption plus a USB drive, but is sometimes slightly higher. However, the hardware-encrypted USB drives typically have longevity and performance in line with premium off-the-shelf USB drives, which can mitigate extra costs here.

# Hardware-Based Versus Software-Based Encryption

## Management, Maintenance, and Ongoing Costs

Maintenance of software encryption means involvement with desktop images, as the software must be installed and maintained. Most software encryption systems do not provide management features, such as the ability to rescue a user who has forgotten their password.

With no software installation, hardware encryption has much lower maintenance costs. Management systems are typically more full-featured, providing for device issuance, asset tracking, and user rescue and/or password reset. More advanced features, such as device revocation, usage restriction to trusted networks, and others are also available with some products.

## Usability

### Functionality

With many software encryption products, users must choose to encrypt data before it's placed on the device. With others, they have to copy data to the device using a special application. In both cases, the convenience of treating the device like any other drive is often lost, sometime leading to users circumventing the security entirely.

Hardware encryption products require identity verification, but afterwards operate just like a normal USB drive – no special applications, and no extra steps. Users can also work directly from a hardware-encrypted device, eliminating any need to store a copy of their data on the local machine – an ability simply not available with most software encryption products.

### Portability

Software encryption requires software be installed on every machine where the user needs to access to the device, an action that usually requires administrative privileges. Hardware encryption requires no software installation, and can be used anywhere the user goes.

### Speed

Hardware encryption is handled with a dedicated on-board processor that can encrypt/decrypt data faster than the CPU in a typical computer. The result is faster data transfer and a smaller burden on the user's computer than is possible with software encryption.

The decision to select hardware-based encryption is only the beginning of a process that includes the evaluation of a number of key product features in an effort to choose the right portable security device.

For additional insight, read MXI Security' whitepaper entitled Choosing the right Portable Security Device available at [www.mxisecurity.com](http://www.mxisecurity.com).