# The Advantages of Hardware-Based Data Encryption

*As new advances in technology emerge, so too do new cybercrime attack vectors. Sensitive data such as financial information, e-mails, PINs, electronic medical records, social security numbers, and payment transactions must be protected. Encryption is widely used and understood as a safe and reliable method of keeping valuable information out of the wrong hands. What is not as commonly understood is that encrypted information is only as secure as the underlying technology protecting it. It is of critical importance that organizations understand the full scope of options available, as well as the unique characteristics of hardware-based data encryption, prior to selecting a solution.*

## The Importance of Data Encryption

At the core of a hardware-based data security infrastructure is encryption technology. Encryption is the process by which sensitive data is rendered indecipherable through the use of secret keys. Encryption keys are the secret values that cryptographic algorithms use to produce this indecipherable data, or ciphertext.

There are two different types of encryption: symmetric and asymmetric. Symmetric means the sender and receiver of a message use the same key to encrypt and decrypt data. Asymmetric involves a public key and a private key: the public key is used to encrypt the data, while only the private key can decrypt the data.

There are also two different methods used for encrypting and decrypting data: hardware and software.

Software-based encryption uses computer applications to protect sensitive data, typically through the use of keys or passwords that are typed directly into the computer. While software encryption can be relatively easy to maintain and allows multiple users to be easily granted access to the encrypted data, it may not always provide the strength and security users might hope for.

Hardware-based data encryption offers organizations significantly greater protection for sensitive data. Encryption tasks are performed by a separate device called a hardware security module, or HSM. An HSM is a dedicated, standards-compliant cryptographic appliance designed to protect sensitive data in transit, in use, and at rest through the use of physical security measures, logical security controls, and strong encryption.

## Hardware Versus Software Encryption: An Overview

Software-based encryption is useful because it can be relatively easy to use, cannot be physically lost or damaged, and is widely accessible. Many organizations use software-based encryption to protect sensitive data such as e-mails and everyday documents. While it can be an acceptable first line of defense, software encryption is not the most reliable form of protection and can often foster a false sense of security.

Hardware-based security is often faster and more efficient than software-based encryption because it operates on a separate device dedicated solely to the purpose of data encryption. This separation adds an additional layer of protection and can dramatically enhance speed. Because of this physical separation, HSMs can also offer advanced disaster recovery and redundancy features in the event of an unplanned outage or loss of network connectivity.

Furthermore, in order to access the clear encryption keys contained within the HSM, attackers must physically tamper with the device, whereas a simple keylogger can often prove the downfall of software-based tools. HSMs, however, are capable of identifying unauthorized access or attempted attacks. Any attempt at tampering with the hardware will cause the device to immediately erase all sensitive data, preventing the attacker from acquiring that information.

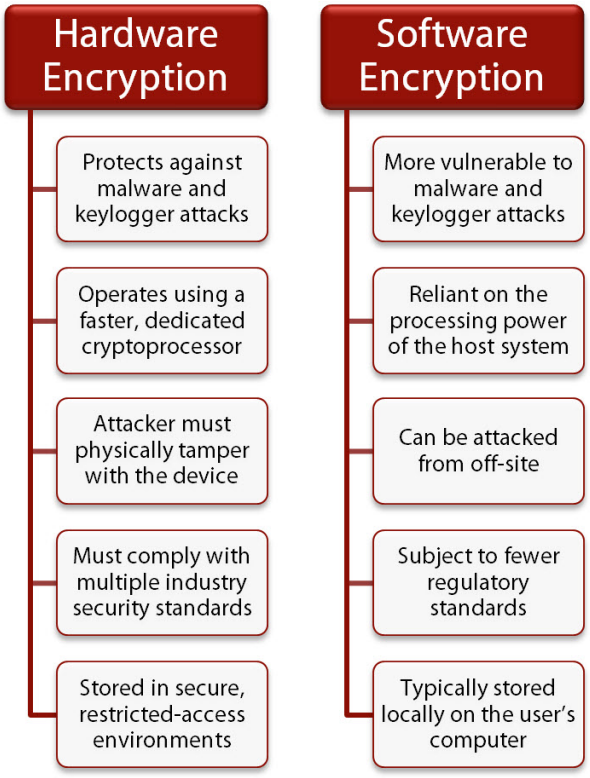
## The Role of Regulatory Compliance

HSMs are held to strict security standards, and different industries often have specific regulatory requirements for their organizations. Three common standards involving hardware encryption solutions are FIPS 140-2, PCI DSS, and PCI HSM.

Federal Information Processing Standards (FIPS) 140-2 is a U.S. government security standard that accredits cryptographic modules used within a security system protecting sensitive information. Cryptographic modules are graded on a scale of 1-4, and it is generally accepted that HSMs must be validated to Level 3 or greater in order to adequately protect sensitive data.

PCI DSS, or the Payment Card Industry Data Security Standard, is a multifaceted set of security requirements for enhancing the security of electronic payments. Any organization that accepts, processes, or stores card-based payment information must comply with the standards set by PCI DSS.

PCI HSM requirements dictate the secure design and deployment of HSMs. To obtain validation, a cryptographic device must meet a set of strict criteria concerning the device's physical and logical security. In addition, requirements regarding the integrity of the device during manufacturing and transit ensure that the device will not be compromised before its initial deployment.




## About Futurex

For over 30 years, Futurex has been a globally recognized name in providing secure, scalable, and versatile data encryption solutions.

More than 15,000 organizations worldwide have trusted Futurex's innovative hardware security modules to provide market-leading technology for the secure encryption, storage, and transmission of sensitive data.

Futurex maintains an unyielding commitment to offering advanced, standards-compliant data encryption solutions alongside world class customer service.

## Uses of Hardware-Based Encryption

The following industries are just a few examples of the many where hardware-based data encryption is currently used.

**Financial** - Banks, credit unions, transaction processors, and other financial institutions use hardware security to protect sensitive customer information such as PINs and account numbers. Hardware security modules help to prevent credit and debit fraud, identity theft, and insider attack.

**Retail** - Merchants, both online and offline, use hardware-based security to protect payment records and card numbers, both while processing and while being stored for later use in returns, chargebacks, and future purchases.

**Healthcare** - Healthcare professionals use hardware-based security solutions to protect sensitive information such as medical records, research conducted at hospitals, confidential insurance documentation, and prescription records while in transit and while being stored.

**Government and Defense** - Government and national defense entities processing sensitive data require versatile, hardware-based encryption platforms with the functionality to secure many different types of information. From securing citizen identity card production to encrypting and storing sensitive records, the benefits offered by hardware security technology are substantial.

FUTUREX

**Global Headquarters** 864 Old Boerne Road, Bulverde, Texas 78163 USA
TF 800.251.5112 P +1 830.980.9782 F +1 830.438.8782 info@futurex.com
**WWW.FUTUREX.COM**