Data Encryption

No matter the size of the business, every organisation relies on the collection and management of data in everyday operations.

Whilst we have become so reliant on data, if it is not properly managed, secured and protected it can quickly become a liability.

What is data encryption?

When dealing with data or information in any capacity, data encryption is your best friend. No matter whether you are dealing with payment information, personal data or trade secrets, the purpose of data encryption is to protect and ensure the confidentiality of data as it is stored on a computer system, database or when it is shared between users.

How does data encryption work?

Data encryption can take shape in a number of different ways depending on the nature and the destination of the file. The modern form of data encryption encrypts data or plaintext through the combination of an encryption algorithm and a subsequent encryption key. The process results in a form of ciphertext, which can only be accessed in its original form when decrypted with the correct key.

Types of encryption

There are two main forms of data encryption businesses can utilise:

Symmetric

Symmetric encryption uses the same dedicated key to encrypt the relevant file or message. Symmetric encryption is widely seen as a faster method of sharing data efficiently, however, it can only work when the sender exchanges the encryption key before the end user can decrypt.

Asymmetric

Referred to as public-key encryption, asymmetric uses two different kinds of encryption keys, one public and one private. Asymmetric encryption is often seen as the preferred option for data encryption due to the fact that both the public and private keys can encrypt a file to assure the confidentiality, integrity, authenticity, and non-reputability of electronic communications and data through the use of digital signatures.

Data encryption with Hyve

We recognise the importance of securing your mission-critical data in everyday business operations. With this in mind, we have developed an industry-leading data encryption service that can be developed to meet the needs of your business.

Database backup encryption

Hyve offers a dedicated database backup encryption service that allows you to backup your data and secure it simultaneously. By creating compressed and encrypted backups of your database, Hyve's database backup encryption service allows you to make smaller, faster and most importantly safer backups at any time. Once the file has been backed-up, the file will be encrypted, securing the file only for people who have designated access.

Features

- Up to three levels of compression, with a compression analyser facility, so you know best whether to optimise for speed or for size

- User-friendly GUI to guide you through the backup and restore processes

- 256-bit encryption to ensure your backups are secure

- Split backups, enabling you to take advantage of multi-CPU and high-speed disk array systems to speed up the backup and restore process even further

File encryption

Hyve offers a dedicated file encryption service that supports best practices for hardening your critical data and securing your data from malicious users. Hyve's file encryption service protects your files from intrusion, protects against viruses or firmware, encrypts sensitive information in log files and secures files by encrypting the underlying files.

Features

- Industry-leading encryption for structured and unstructured data

- Flexible encryption across application programs

- Separation of duties between security administration and system administration

- Customisable alert and reporting formats for compliance requirements

How can Hyve help?

To find out how Hyve can help you keep your data and files secure and allow you to take advantage of our dedicated data encryption service, contact our sales team today.