

ENVAULT™ Encryption Method

PROBLEM: USER PASSWORDS FAIL TO PROTECT YOUR COMPANY DATA AGAINST THEFT AND LOSS

Current mainstream encryption products often rely on a single secret encryption key to protect an entire disk partition. Encryption keys are generally derived from user passwords that are often weak and vulnerable to dictionary attacks via exhaustive search.

Such an attack is essentially undetectable; an adversary may simply copy the contents of the disk, return the device to its owner and perform the attack offline.

The attacker can obtain the user passwords also through e.g. social engineering, shoulder surfing or keyloggers. Disclosure or breaking of the secret encryption key will irrecoverably yield all information to the attacker, while the victim of data theft (the organization) has no way of knowing of the occurrence of the theft.

In worst case, the attacker comes from inside the organization - a disgruntled employee knows his own passwords to the disk, so there is nothing to keep him or her from taking the data outside your organization - for example to a competitor.

Therefore, relying on user passwords when encrypting an organization's data does not provide the desired protection against data leaks and theft.

SOLUTION: WE NEED PASSWORD-FREE AND AUTOMATIC ENCRYPTION WITH REMOTE CONTROL AND AUDITING CAPABILITIES

To counter the inherent problems with traditional solutions, Envault Corporation has developed the unique and patent-pending Envault™ encryption method.

In Envault encryption, the data protection is based on encryption combined with data distribution and centralized key management. All decisions and complexity are hidden from the end-user, and a special software takes care of the encryption and decryption processes transparently.

The end-user can continue working just as before. The encryption system processes files in the background and provides the secret keys on-demand if and when access conditions are met.

Access conditions (user authentication, location, network connection, time etc.) are centrally managed by the organization. An Envault encrypted file can for example be accessed only on known corporate computers, or it can be made to be readable outside the organization only for X days.

To prevent data theft and to provide an efficient method for document lifecycle management, the Envault encryption has built-in remote suspend/kill and file tracking/auditing capabilities. A protected document can be suspended from any location, without any connection to the storage device it resides on.

THE METHOD IN A NUTSHELL

A plaintext file is first encrypted and then divided into two parts by removing bits (entropy). The parts are stored in separate locations: One on the disk, and the other in a central location that the organization can control. Each part alone contains just useless noise, but when combined together, the parts form the original plaintext file. The distribution ratio is typically 99.5:0.5.

Remote access control: Organization defines who, where and when can get the centrally stored part. Without it, nobody can read the file contents.

Auditing: Each file write and read generates an access to the centralized storage, allowing an indisputable audit trail.

THE ENCRYPTION PROCESS

Figure 1 shows the Envault process. The steps are as follows:

Inner Diffusion and Primary Encryption:

In Inner Diffusion and Encryption a data block is encrypted via a pseudo-random permutation (PRP) specified by a secret, random key using AES-256. A special mode of operation is used that guarantees that each output bit depends on each key and input bit.

Entropy removal:

In the Entropy Removal step a small number of entropy bits of the diffused block R is removed and stored into a centralized, trusted server controlled by the owners of the data (corporation, government body or other such organization) using a secure SSL link. Reconstruction of any portion of the original input block is unfeasible without this information. The removed data R also uniquely identifies the contents of the entire data block.

Outer Diffusion and Secondary Encryption:

After entropy removal, the data block is further encrypted and diffused using AES-256. The secondary encryption process also guarantees that known/chosen ciphertext attacks are as unfeasible as known/chosen plaintext attacks.

COMPLIANCE INFORMATION

The main security standards that apply to envaulting are:

Confidentiality: AES-256 (FIPS 197, FIPS 140-2) is used for encryption and diffusion. AES has been approved by NSA for up to TOP SECRET information in federal use when used with a 256-bit secret key.

Communications security: The SSLv3 or TLS is used for client-server communication. The SSLv3 authentication certificates are issued by Envault's own secure PKI CA.

Authentication and access control: The novel remote control feature of a storage device is based on patent-pending technology developed by Envault Corporation. Authentication in transport (SSL) is based on industry-standard PKI mechanisms.

Key generation: The nondeterministic key generation mechanism fully meets the criteria set in FIPS 140-2

In addition, Envault fulfills all the relevant security requirements set in the Payment Card Industry Data Security Standard (PCI DSS), SOX and HIPAA.

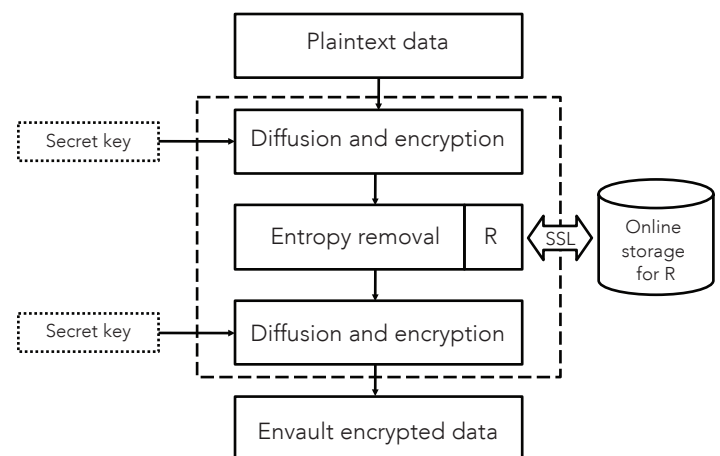


Fig. 1: The encryption process



INSIDE

SALES CONTACT

Email: sales@envaultcorp.com
Tel.: +358 (0)9 3540 1888

SUPPORT CONTACT

support@envaultcorp.com
+358-(0)40-143 5320

WEB

www.envaultcorp.com