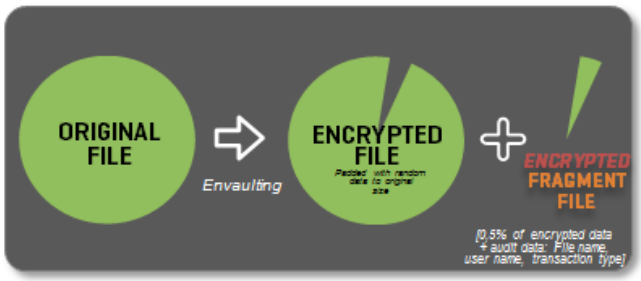
ENVAULT double guard FILE PROTECTION

KEY BENEFITS

Fast & easy centralized deployment and management: Client deploys with silent MSI installation. Encryption rules are flexibly managed through Active Directory Group Policies (ADM template).
Easy to use: No user training is required as the encryption is transparent to users and protected Data works just as before.
Centralized key management - no password recovery required: Fragmentvault-server centrally manages the encryption keys per file. AD login/password combination is used for user authentication. Lost password can be reset through AD.
High performance & manageability: Computer boots up quickly and stays responsive as the operating system is not encrypted. System maintenance, backup or restore is easy for IT admins as they can login as local admin.
Low Total Cost of Ownership: License cost is usually only a part of the total lifecycle costs of a software solution. Envault makes sure that deployment and running costs are minimized and all overhead is eliminated.

ENVAULTING METHOD

Technology Patented in EU and US



KEY FEATURES

Ultra-strong Envault encryption:

Confidentiality: AES-256 (FIPS 197, FIPS 140-2) is used for encryption and diffusion.
Communications security: TLS is used for client-server communication. The TSLauthentication certificates (X509v3 RSA/SHA2) are issued by Envault's own secure PKI CA. Customer's own certificates may also be used.
Authentication and access control: The novel centralized data remote control feature is based on patent-pending technology developed by Envault Corporation. Windows AD login/password combination and Kerberos authentication is used for authenticating user on Windows. Authentication in transport (SSL) is based on industry-standard PKI mechanisms.
Key generation: Nondeterministic key generation mechanism fully meets the criteria set in FIPS 140-2.
Targeted protection for the payload: You can protect user writable partitions/folders and leave the operating system (overhead) outside. File-based protection gives you greater control and does not slow down your PC's performance or startup times like full disk encryption.
Flexible security policy management through Active Directory: Enforce data protection and make user group specific rules for offline use.
File transaction based audit trail and use statistics: Fragmentvault audits all file transactions and builds graphic usage statistics allowing easy reporting and tracking of files, data volumes and device count. Allows seeing exactly what is
stored on laptops and showing that your confidential data is encrypted.
Remote suspend/kill for PC contents through Envault Manager console: One click to neutralize a lost or stolen laptop.

COMPLIANCE

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 TLS is used for client-server communication. The TSL 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.

ENVAULT

SALES CONTACT
sales@envaultcorp.com
+358 (0)40 500 6514

ENVAULT CORPORATION
Tekniikantie 12
FI-02150 Espoo, Finland

WEB
www.envaultcorp.com