

ENVAULT™ Internal Disk Protection

SMART & CENTRALLY MANAGED ENCRYPTION, REMOTE CONTROL AND AUDITING FOR YOUR CONFIDENTIAL DATA ON INTERNAL HARD DISKS

Envault™ Internal Disk Protection software lets you easily protect your confidential information stored on company PCs against theft and loss. You can smartly target the centralized Envault encryption to the actual 'payload', instead of encrypting the full disk.

PROTECTED PC:



User partition (e.g. D:\ or E:\)

Payload protection: Envault encrypts all files and folders on the protected partition. The encrypted data is under remote control & auditing. Access requires valid Active Directory login or a smart card.



System partition (e.g. C:\) :

Payload protection: Envault encrypts a desired folder on system drive. The encrypted data is under remote control & auditing. Access requires valid Active Directory login or a smart card. Operating system (C:\Windows) is not encrypted.



AD Security policy:

Standard user can write files only to protected partition / folder.

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 PC 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.



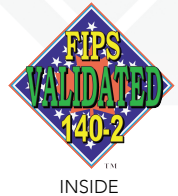
INSIDE

KEY FEATURES:

- Ultra-strong Envault encryption:
 - 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: SSLv3 or TLS is used for client-server communication. The SSLv3 authentication 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:

Envault encryption and auditing fulfills all relevant security requirements set in the Payment Card Industry Data Security Standard (PCI DSS), SOX and HIPAA privacy rules. A FIPS 140-2 Validated crypto module is used inside the Envault software.



SYSTEM REQUIREMENTS:

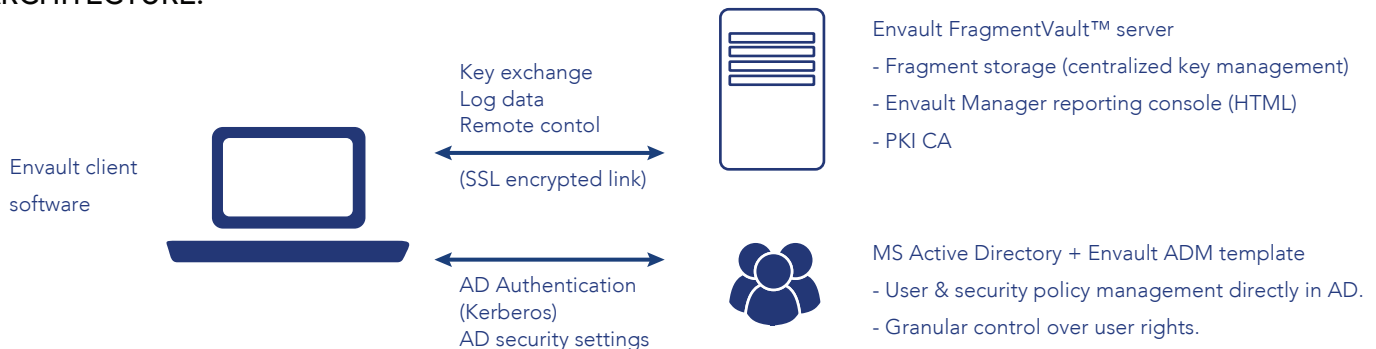
FragmentVault™ server:

- Linux (RedHat, CentOS) or Windows Server 2003/2008 platform on either physical machine or virtual machine.
- Minimum hardware specs: system memory 4 GB, internal disk 100 GB and a Gigabit grade network interface card.

Envault™ Internal Disk Protection client:

- Microsoft Windows XP SP3 (32 bit), Vista (32 & 64 bit) and Windows 7 (32 & 64 bit)
- Minimum system memory 256 MB, 50 MB internal disk + configurable cache size.

ARCHITECTURE:



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