

ENVAULT™ Removable Media Protection

DEVICE CONTROL, SMART ENCRYPTION, DATA LIFECYCLE MANAGEMENT AND AUDITING

Envault™ Removable Media Protection software lets you easily protect your confidential information stored on removable media such as USB flash drives, external USB/FireWire hard disks and other storage devices that can be attached to corporate computers. Software-based encryption works with your existing devices, so no special hardware is required.

FLEXIBILITY & EASE OF USE: ALL USE CASES SUPPORTED



DEVICE GETS TWO ZONES WITH DIFFERENT ACCESS RULES:

- 1) Envaulted zone for company internal use, and
- 2) Temporary Airlock™ zone for exchanging files with external users.



+



ONLINE: All files accessible.



+



OFFLINE: Recent Envaulted files & all Airlocked files accessible within time limit.

@customer



+



3RD PARTY COMPUTER:
All Airlocked files accessible within time limit.
Pssphrase authentication possible.

CONTROL & VISIBILITY LIKE NEVER BEFORE



Security rules set and managed through an Active Directory Group Policy template



Lifecycle management: Remote suspend / kill devices and data



Log & audit all file transactions and device use, online & offline

KEY BENEFITS

- Fast & easy centralized deployment and management: Client deploys with silent MSI installation. Encryption and device control 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 media works just as before in your corporate PCs and network.
- Centralized key management - no password recovery required: FragmentVault server centrally manages the encryption keys per file.
- High performance: Initialization of new storage media takes only a few seconds.
- 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.



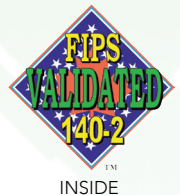
INSIDE

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. Customer's existing infrastructure 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.
- Flexible security policy management through Active Directory: Enforce data protection, whitelist/blacklist devices 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 removable media and showing that your confidential data is encrypted.
- Remote suspend/kill for devices and data through Envault Manager console: One click to neutralize a lost or stolen device.

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 50 GB and a Gigabit grade network interface card.

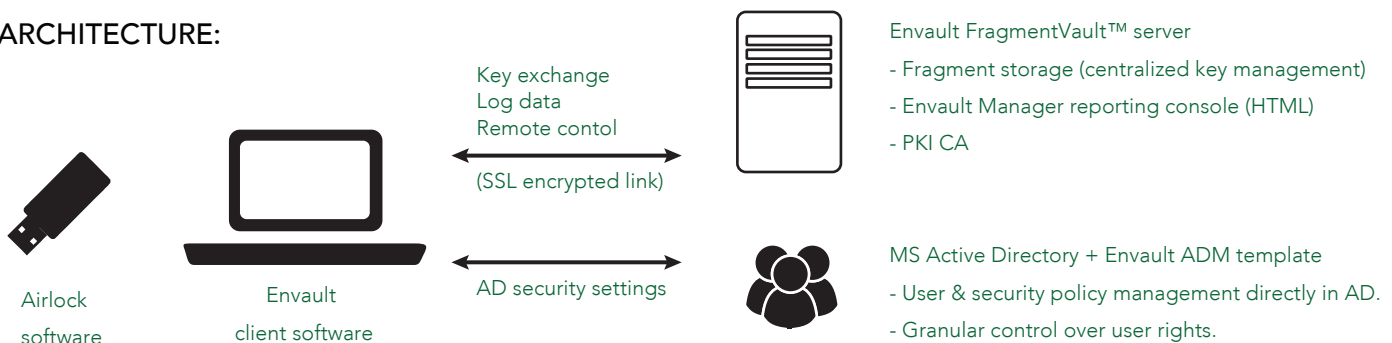
Envault™ Removable Media Protection client:

- Microsoft Windows XP SP3 (32 bit), Vista (32 & 64 bit) and Windows 7 (32 & 64 bit)
- User application available for Mac OS X & Linux (including but not limited to RedHat, CentOS, Ubuntu)
- Minimum system memory 256 MB, 50 MB internal disk + configurable cache size.

Envault™ Airlock software:

- Microsoft Windows XP or better, Mac OS X or Linux (including but not limited to RedHat, CentOS, Ubuntu)

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