Pointsec® Media Encryption

Pointsec® Media Encryption automatically, and in real-time, protects information wherever it is. Whether stored on memory sticks, storage media or in transit – Pointsec Media Encryption's transparent, strong, FIPS-certified encryption ensures that information is only accessible to those who should have access to it.

The use of removable media, such as memory cards and sticks, is increasing. Nowadays, huge amounts of sensitive information can be carried literally in the palm of your hand stored on a USB memory stick. Do you know how many memory sticks are in use at your organization? Do you know what information they contain or how that information is being protected?

With Pointsec® Media Encryption's FIPS-certified, strong encryption – no user intervention required – information is secure whether stored on removable media, floppy disks, locally on a workstation or in transit via e-mail. Moreover, information is still protected when it leaves your organization. Recipients of protected information do not need Pointsec Media Encryption installed; with self-extracting files and stand-alone access all that is needed is the correct password; the software is included.

Other security components such as standard-compliant information deletion guarantee that information cannot be recovered after its lifespan. Central management enables deployment of Pointsec Media Encryption with the minimum of effort and Remote Help ensures users can access information even if they have forgotten the password.

FEATURES/BENEFITS

- **Immediate protection – transparent encryption**
  - Immediately and transparently encrypts all information stored on removable media, floppy disks, local files and folders as specified in the security profile.
  - Supports FAT, FAT32 or NTFS file systems, including USB, USB2/PCCARD/Firewire memory cards, storage media and floppy disks.

- **Central management and Remote Help**
  - Administrator can force encryption on media based on media type (e.g. floppy disk, other removable media), file type (extensions), or directory structure.
  - Using a secure challenge/response procedure, locked users can call their helpdesk to reset their password and regain access to information.

- **Fast and strong, FIPS-certified algorithms**
  - FIPS 140-2 certified cryptographic modules to choose from.
  - Strong encryption using industry standards.

- **Standards-compliant secure file deletion**
  - Secure file deletion in accordance with US Department of Defense standards.

- **User-friendly**
  - Instant encryption using standard Windows menus and button clicks.
  - Self-extracting files for e-mail, no need for the recipient to have Pointsec Media Encryption installed.
  - Single Sign On with Pointsec® for PC. When used with Pointsec for PC, no additional user interaction is required to access encrypted files.
  - Fully transparent to end-users. Once logged on, a double-click opens a file.
  - Stand-alone access ensures secure distribution of information even if Pointsec Media Encryption is not installed.

● pointsec

Immediate protection – transparent encryption

Pointsec Media Encryption's on-the-fly encryption protects information immediately, whether it's on a memory card, storage media or a hard disk.

The FIPS-certified AES algorithms used by Pointsec Media Encryption ensure fast and strong encryption of all information with no discernible reduction in speed or performance. If you use Pointsec for PC, Pointsec Media Encryption's Single Sign On means that no additional interaction is required to access protected information.

Central administration

Central administration is a requirement for any enterprise, no matter what software solution is being deployed.

With Pointsec Media Encryption, administrators can create, deploy, manage, and update their organization's security policy for removable media from one central location. This includes: which information should or should not be encrypted, password length and strength, and maximum number of failed authentication attempts. Central administration also ensures that the security policy is enforced.

Remote Help

Remote Help is a must when deploying security software to thousands of mobile devices. Pointsec Media Encryption enables the user to securely regain access via Remote Help if they are denied access to their information as a result of forgetting their password.

Administrators and authorized helpdesk staff can help the user via a secure challenge/response procedure, enabling the user to quickly regain access to the information, re-set the password, and continue working. Remote Help does not require network connectivity.

Complete mobile security

Distributing information securely is always possible with Pointsec Media Encryption – recipients do not even need to have Pointsec Media Encryption installed.

Information can be distributed in self-extracting files or with stand-alone access. A self-extracting file contains both the information and the software needed to decrypt the information. Stand-alone access provides the recipient with an easy-to-use wizard to decrypt the information. The wizard also enables the secure updating or deletion of protected information.

As part of Pointsec's family of security products for the mobile enterprise, Pointsec Media Encryption provides the most complete, integrated security solution for removable media on the market.

Pointsec media encryption minimum requirements
• Windows 2000/XP
• 64 MB RAM

www.pointsec.com