

## Benefits

Secures files on servers, laptops, workstations, and portable media without impacting user productivity

Easy, and transparent-to-end users, integration into existing PKI environments

Also secures data files in transit through the LAN and WAN

Secure user group access to encrypted files/folders

No user training required

No noticeable performance loss

Automatic silent mass deployment capability

# SafeNet Data-at-Rest Protection ProtectFile™

## File and Folder Encryption

### Addressing Threats to Data

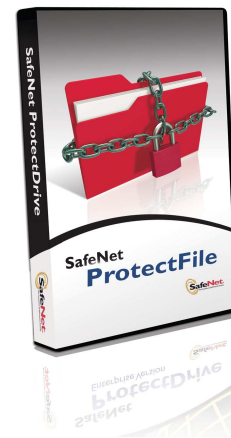
SafeNet ProtectFile addresses data security through fully automated encryption of files and folders stored on servers, network drives, workstations, laptops, and removable media.

Once a user has been successfully authenticated during the Windows log-in process, ProtectFile is initiated automatically, without any additional steps necessary, making the solution easy for end users. Cryptographically-enforced user and group permission-based access ensures that only properly authenticated users have access to confidential data.

ProtectFile integrates seamlessly into the Windows client environment. All documents in a secured folder are encrypted and decrypted automatically and transparently when users open and save files from within applications, or double-click, copy, paste, or move them in the File Explorer.

In fact, ProtectFile is so easy to use that no general user training or change of application operating behavior is required. ProtectFile is available in two versions — each optimized for PKI and non-PKI infrastructures respectively.

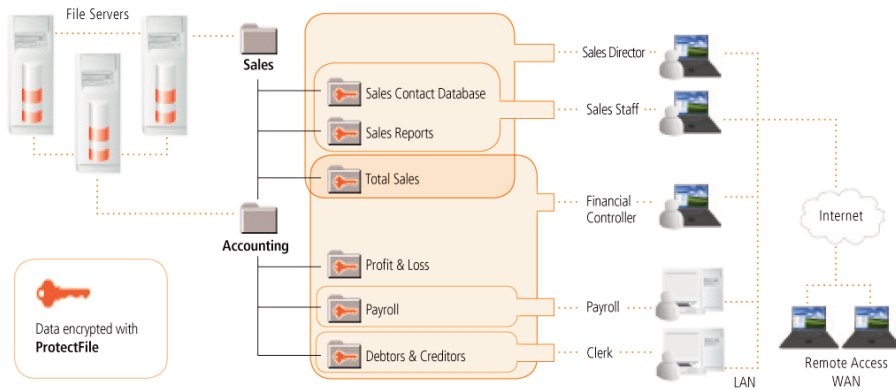
- ProtectFile Premium (PKI) – works with X.509 v3 certificates using an X500 Directory and an existing Public Key Infrastructure (PKI) environment to manage users and certificates.
- ProtectFile Business – is designed for use in non-PKI environments, optionally utilizing a built-in Central Management Console for user profile management, and creation of user groups and individual users, along with the recovery of keys and encrypted files/folders.



### Typical Applications

Typical uses of SafeNet ProtectFile include the following:

- Provides secure user group access to centrally stored and sensitive confidential data, such as customer files, payroll, financial information, strategic plans, etc.
- Eliminate the risk of malicious interception of confidential information that is in transit across the LAN.
- Securing access to confidential data stored on Application Service Provider (ASP) facilities. As data is secured at client level, confidential data is protected not only on the outsourced storage server, but also in transit between the ASP and the computing devices remote location.
- ProtectFile is often used as part of an overall solution to assist adherence to legislated privacy laws that require organizations to secure electronic information on customers and employees.
- ProtectFile's ability to control access to encrypted files that are stored anywhere within the local area network, on mobile devices, and on portable storage media, secures privacy-related information from unauthorized exposure. Since encryption and decryption is undertaken on the client, the savvy hacker is unable to intercept such confidential data as it traverses the network.



## Easy Deployment and Management

Rapid and low-cost deployment in both large and small environments is facilitated by remote silent installation and a scripting interface. Remote installation automatically sets client configurations with pre-definable security policies. A scripting interface facilitates streamlined deployment incorporating automatic mass configuration of encrypted folders, including the addition and removal of secured folders and user access.

A benefit unique of ProtectFile is the ability for user group managers to control the access rights within their user group to encrypted file folders relevant to their area of responsibility. This separates the management of the system from its security, reducing the burden on, and liability of, network administrators. The creation and day-to-day management of encrypted folders is streamlined through a user-intuitive ProtectFile GUI (Graphic User Interface). This facilitates easy creation and deletion of encrypted folders, along with user and ProtectFile administrator control.

## High-Strength Encryption and Authentication

ProtectFile has been designed and built to meet today's demanding security requirements using the latest security best practices and technologies. Major security features incorporated into the design include:

- The latest and proven cryptographic algorithms are used to encrypt all data files, temporary files, and authentication keys whether stored on computing devices or in transit through the LAN and WAN as they are retrieved from data appliances.
- Increased security is delivered by user access being authenticated with both a passphrase (something only the user knows) and the physical insertion of a smart card or USB token (something only the user has) into the device.
- Data files are transparently encrypted at the client computing device before being transferred to file servers. System administrators can maintain and backup the files/folders, but cannot view the contents of the files without appropriate access authentication.
- Decryption keys are secured from unauthorized access by storing them in an encrypted form. Only the correct authentication can unlock the key to decrypt data.

## Technical Specifications

### File and Folder Encryption

- Hard drives of local and remote servers, network drives, workstations and laptops
- Removable media (CD-ROM, USB, floppy...plus more)
- File servers (Microsoft and Novell, Netware, Unix [Samba], more)
- Automatic Temporary file encryption
- Optional Page File encryption

### Encryption Algorithms

- 3DES, IDEA, AES-128, AES-192, AES-256

### Supported Platforms

- Microsoft Windows 2000, XP, and 2003 server 6MB of free disk space

### Interoperability

- Microsoft Windows Terminal Server, Offline Folder Synchronization, DFS (Distributed File System), Global Catalog, Citrix Terminal Server, and Novell
- Easy integration into existing PKI environments (Entrust, RSA, Microsoft, and others) enables advanced key backup, recovery, update and management, plus user access control

### Software Management Tool

- RIS, SMS, Tivoli, TNG, Active Directory, plus many more

### Multi-factor Strong Authentication

- Virtually all tokens and smart cards with PKCS#11, Microsoft CSP, or Vasco Digipass

**Corporate Headquarters:** 4690 Millennium Drive, Belcamp, Maryland 21017 USA  
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524, Email: [info@safenet-inc.com](mailto:info@safenet-inc.com)

**EMEA Headquarters:** Tel.: + 44 (0) 1276 608 000, Email: [info.emea@safenet-inc.com](mailto:info.emea@safenet-inc.com)

**APAC Headquarters:** Tel: +852 3157 7111, Email: [info.apac@safenet-inc.com](mailto:info.apac@safenet-inc.com)

For all office locations and contact information, please visit [www.safenet-inc.com/company/contact.asp](http://www.safenet-inc.com/company/contact.asp)

[www.safenet-inc.com](http://www.safenet-inc.com)