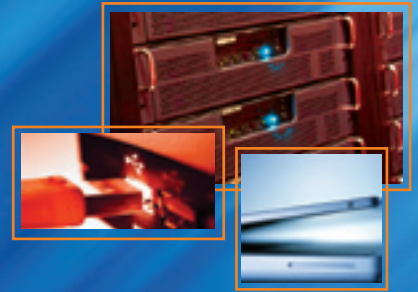


ProtectFile

File Encryption



SafeNet Borderless Security ProtectFile delivers fully automated file encryption and permission-based access to protect sensitive information stored on servers, network drives, workstations, laptops and portable media.



SafeNet Borderless Security ProtectFile encrypts files and folders whilst cryptographically enforcing user and group permission-based access to confidential data.

Internally, data security risks have escalated in recent years due to the practice of storing data on network attached devices (file servers, workstations and laptops) and the growing use of high capacity portable media (memory sticks, CDs and DVDs). Similarly, the level of external threats has also increased as the result of outsourced data storage and system administration.

ProtectFile enables the ability to easily control individual and group permission-based access to encrypted data that is stored on various devices throughout an organization.

Fully automated file encryption delivers the ultimate level of security to local and remote files/folders on servers, network drives, workstations, laptops plus portable media (USB Memory Sticks, CDs, DVDs to mention a few). **ProtectFile** encrypts and decrypts data at the client ensuring protection of confidential files in transit through the LAN or WAN, minimizing opportunities for data thieves who monitor network traffic.

ProtectFile is so easy to use that no general user training or change of application operating behavior is required. All documents in a secured folder are encrypted and decrypted automatically and transparently by **ProtectFile** when users open and save files from within applications, or double-click, copy, paste or move them in the File Explorer.

A benefit unique to **ProtectFile** is the ability for user group managers (termed **ProtectFile** Administrators) to control the access rights within their user group to encrypted files/folders relevant to their area of responsibility. This separates the management of the system and its security reducing the burden on, and liability of, network administrators.

SafeNet Borderless Security ProtectFile is available in two versions:

- **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** - designed for use in non-PKI environments, optionally utilizing an inbuilt Central Management Console for user profile management and creation of user groups, individual users, plus the recovery of keys and encrypted files and folders.

BENEFITS AT A GLANCE

SECURITY

- Secure files on servers, laptops, workstations and portable media without adversely impacting the productivity of authorized users
- **ProtectFile** secures data files in transit through the LAN and WAN
- Secure user group access to encrypted files/folders
- Easy integration into existing PKI environments

USABILITY

- No user training required
- No Right Clicks - A right click command, or any other specific **ProtectFile** command, is not required to initiate encryption or decryption
- Single sign-on to the Windows environment
- No noticeable performance loss

MANAGEABILITY

- Centrally or decentrally control user-group access rights to encrypted files/folders relevant to their areas of responsibility
- Easy and cost effective large scale deployments can be achieved utilizing existing Windows user management systems and strong scripting capabilities
- No need to individually set up user access profiles after automatic silent mass deployment of **ProtectFile**. User profiles can be pre-allocated from a central management console to allow access to designated encrypted files

PRODUCT DATA SHEET



ProtectFile = Ultimate Security

ProtectFile encrypts files and folders stored on, or traveling between servers, workstations, laptops, plus portable devices and media. Using the latest proven encryption algorithms, the ultimate level of security is provided against the most advanced hackers and data thieves.

Security Features	Security Benefits
File and folder encryption	Files and folders can be protected on: <ul style="list-style-type: none"> ▪ The 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], plus more)
Encryption algorithms 3DES, AES-128, AES-192, AES-256, IDEA	ProtectFile encrypts all data files and authentication keys using industry proven cryptographic algorithms, securing files stored on computing devices and in transit through the LAN and WAN as they are retrieved from data appliances.
Encrypted network traffic	ProtectFile ensures confidential data files are encrypted and protected in transit through the LAN and WAN as applications retrieve stored encrypted data. This is possible due to encryption and decryption occurring on the client.
Multi-factor/strong authentication	Increased security is delivered by user access being authenticated with both a pass-phrase (something only the user knows) and the physical insertion of a smart card or USB token (something only the user possesses) into the device.
Secure file servers	ProtectFile transparently encrypts data files 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.
Secure key storage	ProtectFile protects decryption keys from unauthorized access by storing them in an encrypted form. Only the correct authentication can unlock the key to decrypt data.
Automatic Page File encryption	By optionally encrypting the Windows Page File, ProtectFile denies hackers the opportunity to access sensitive data in the clear when it is temporarily swapped out from physical memory to the page file on the hard drive.
Automatic Temporary File encryption	Automatic encryption of files in the shared Windows temporary folder, utilizing user-specific cryptographic keys, ensures privacy of data for individual users when temporarily stored on the hard drive by applications.



ProtectFile = Ultimate Usability

ProtectFile delivers the ultimate level of usability requiring no application training for the user. This enables rapid adoption throughout an organization, an important consideration where the number of users is high.

Usability Features	Usability Benefits
Transparent data encryption and decryption	No Right Clicks - A right click command, or any other specific ProtectFile command, is not required to initiate encryption or decryption. All files in a secured folder are encrypted and decrypted automatically and transparently without any additional interaction by the authenticated user. Authenticated users will only be granted decryption access to files that they have the pre-allocated rights to view and use.
Single sign-on	Once the user has been successfully authenticated during the Windows log-in process, ProtectFile is initiated automatically without any additional need for authentication.
Minimal performance loss	No noticeable delay occurs during encryption operations with ProtectFile and only 6Mb of hard drive space is required. ProtectFile does not adversely impact upon server performance as all encryption and decryption is performed at the client level.



ProtectFile = Ultimate Manageability

ProtectFile delivers the ultimate level of administration management throughout IT environments of all sizes. A track record of successful deployments of over 10,000 seats in a single installation proves its flexibility and scalability.

Manageability Features	Manageability Benefits
Silent network-wide installation	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.
User management API	A user management API enables customers to easily integrate ProtectFile's user management functionality into their own management tools. This reduces the knowledge and skill set deficiencies commonly experienced when introducing a new technology into an organization.
Encrypted folder administration GUI	The creation and day to day management of encrypted folders is streamlined through a user intuitive ProtectFile GUI (Graphic User Interface). This facilitates the easy creation and deletion of encrypted folders, plus user and ProtectFile administrator control.
Transparent key management	ProtectFile automatically takes full responsibility for key management within the computing device. This ensures all key management processes are completed without the possibility of human error. This relieves the burden on administrators and users when adding and removing users, adding new devices or changing configuration settings.
Interoperability	ProtectFile will seamlessly integrate and operate with Microsoft Windows Terminal Server, Offline Folder Synchronization, DFS (Distributed File System), Global Catalogue, Citrix Terminal Server and Novell.
Public Key Infrastructure (PKI)	Seamless integration with Entrust, RSA, Microsoft and various other PKI environments enables advanced key back up, recovery, update and management, plus user access control.
File structure consistency	File and folder names will not change after ProtectFile encryption and there are no folder size restrictions. This ensures changes to existing folder structures do not occur upon automated encryption or when setting up an encrypted folder.



Network-based file and folder encryption incorporating authenticated access management

ProtectFile enables the ability to control individual and group permission-based access to encrypted data that is stored on various devices across an organization.

