



SAFENET PROTECTFILE

PRODUCT BRIEF

Benefits

Growth enabled—

- Pursue new opportunities with the confidence that data is secured across all endpoints.

Collaboration secured—

- Collaborate with business partners knowing that only authorized, authenticated users can view sensitive data.

Productivity empowered—

- Encrypt information transparently, without disrupting business operations, computing performance, or the end-user experience.

Data protection should not end with the data center. Whether you work in retail, manufacturing, financial services, healthcare, energy, or government, you need to make sure you protect sensitive corporate and customer information wherever it resides—from the data center to the wide variety of endpoints used by employees and business partners.

SafeNet ProtectFile software delivers persistent security of unstructured data throughout its lifecycle, from inception to storage. Working together with a SafeNet DataSecure appliance, ProtectFile combines encryption and access control policies to protect the folders and files residing on servers, network drives, desktops, laptops, and removable media. By selecting ProtectFile, you can facilitate collaboration and new modes of productivity with the confidence that your files will all remain secure.

Integrated security, comprehensive coverage

ProtectFile is deployed in tandem with a SafeNet DataSecure appliance, offering an unparalleled combination of broad coverage, robust security, and scalability. ProtectFile encrypts sensitive data in a wide range of flat file types, such as word processing documents, spreadsheets, images, designs, and more.

Centralized administration

The DataSecure appliance provides centralized key and policy management, simplifying administration and tightening security. Administrators can set policies to lock down particular folders and files, granting access only to authorized individuals. When a folder is selected for protection, any file that is deposited in the folder is automatically encrypted.

Transparent operation

Encryption is seamless and transparent with ProtectFile, so there is no disruption to business operations, application performance, or the end-user experience. Once a user has been successfully authenticated, ProtectFile is initiated automatically, applying policies without affecting productivity.

Portable, user-based encryption

With the ProtectFile portable capabilities, enterprise employees also gain the ability to encrypt the files that they create and share without requiring administrator intervention. The employees set authorization policies to determine who can access information. By enabling employees to protect the files they send through e-mail, store on network drives, or share through removable media, ProtectFile provides the portability needed to help boost productivity and provide the confidence to deepen collaboration.

Features

Proven cryptographic algorithms—Provide reliable encryption of all data files, temporary files, and authentication keys, whether stored on endpoint devices or in transit, by using proven cryptographic algorithms.

Technical Specifications

File and folder encryption

- Hard drives of local and remote servers, network drives, workstations, and laptops
- File servers (Microsoft and Novell, Netware, UNIX [Samba], more)
- Remote silent installation for easy deployment in any size environment

Encryption algorithms

- FIPS 140-2 AES

Supported platforms

- Microsoft Windows and Linux

Interoperability

- Microsoft Windows Terminal Server, Offline Folder Synchronization, DFS (Distributed File System), Global Catalog, 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 techniques
- Virtually all tokens and smart cards with PKCS#11, Microsoft CSP, or Vasco Digipass

Supported two-factor authentication

- SafeNet eToken, iKey®, and U.S. DoD Common Access Card (CAC)

Controlled access—Ensure regulatory compliance and reduce risks by setting policies for separation of administrative duties.

Remote installation—Achieve rapid and cost-effective deployment in both large and small environments by using remote silent installation and a scripting interface.

User-driven encryption—Enable your employees to contribute to data protection by allowing them to encrypt the data they create and share.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: www.safenet-inc.com/connected

©2010 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. PB-ProtectFile(EN)-09.10.10