THE
DATA
PROTECTION
COMPANY

SafeNet ProtectFile

PRODUCT BRIEF

Highlights

Transparent, Strong, and Efficient Encryption

- Protect sensitive data-at-rest on servers in the distributed enterprise with transparent and automated file-system level encryption
- Manage encryption keys centrally and securely in FIPS certified hardware
- Apply granular policies based on users and groups, file types, and processes for increased control over high value data

Privileged User Control

- Minimize insider threats by enabling privileged users, such as root or system administrators, to perform authorized duties while keeping sensitive data encrypted and secure

Secure Archival of Data

- Keep high value data encrypted and inaccessible to server administrators performing scheduled back-up and restore tasks

Secure Data Destruction

- Ensure all secured, sensitive data is rendered unreadable in the event destruction of data is required

Easy Implementation and Management

- Utilize remote, silent installation scripts for quick and easy deployment in large and small environments
- Streamline administration and reduce overhead with centralized policy and key management
- Scale cost-effectively as business needs grow

Achieve Compliance

- Meet compliance mandates that require encryption of data and separation of duties

Today, perimeter-based security defenses cannot adequately secure the growing volume of sensitive data residing on servers in physical, virtualized, and cloud-based storage environments. The traditional perimeter no longer exists, and new points of vulnerability have surfaced as a result. To be completely protected, organizations must employ a solution that attaches security to the data itself.

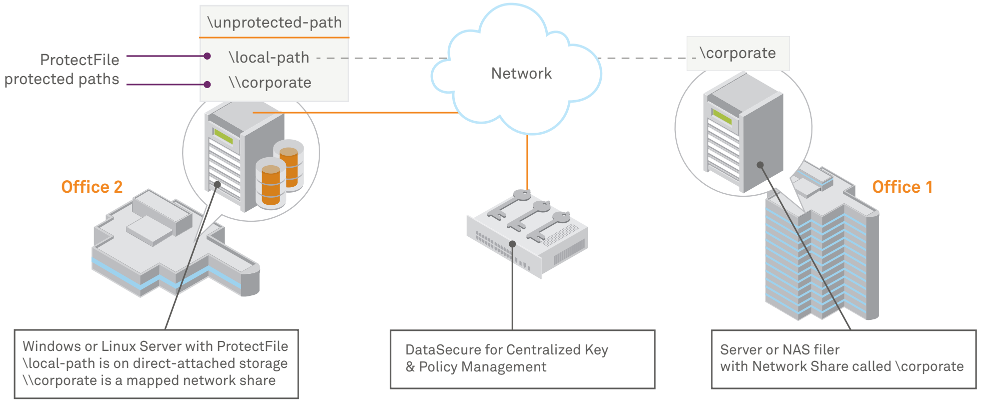
SafeNet ProtectFile ensures sensitive data-at-rest on servers in the distributed enterprise is protected with transparent and automated file-system level encryption, granular access controls, centralized policy and key management, and comprehensive auditing capabilities.

Due to its volume and relevance, high value data on enterprise servers is the most attractive and easily targeted. ProtectFile enables data-centric security by rendering files containing sensitive data useless in the event of a breach, misuse or hijacking of privileged accounts, physical theft of servers, and other potential threats.

Secure Sensitive Server Data-at-Rest in the Distributed Enterprise

ProtectFile is deployed in tandem with SafeNet's FIPS 140-2 Level 3 certified DataSecure hardware appliances for centralized key and policy management, providing robust security and scalability. ProtectFile encrypts sensitive data on servers, such as credit card numbers, personal information, logs, passwords, configurations, and more in a broad range of flat files, including word processing documents, spreadsheets, images, designs, database files, exports, archives, and backups.

Once deployed and initiated on a server, ProtectFile transparently encrypts and decrypts data in local and mapped network folders at the file-system level based on policies defined in DataSecure – without disruption to business operations, application performance, or end-user experience.


\unprotected-path
ProtectFile protected paths
\local-path
\\corporate
Network
\corporate
Office 2
Office 1
Windows or Linux Server with ProtectFile
\local-path is on direct-attached storage
\\corporate is a mapped network share
DataSecure for Centralized Key & Policy Management
Server or NAS filer with Network Share called \corporate

Technical Specifications

File-system Level Encryption

- Servers: A file server, web server, application server, database server, or other machine running compatible software
- Network Shares: SMB/CIFS, NFS
- Remote silent installation for easy deployment in any size environment

Encryption algorithms

- AES

Supported platforms

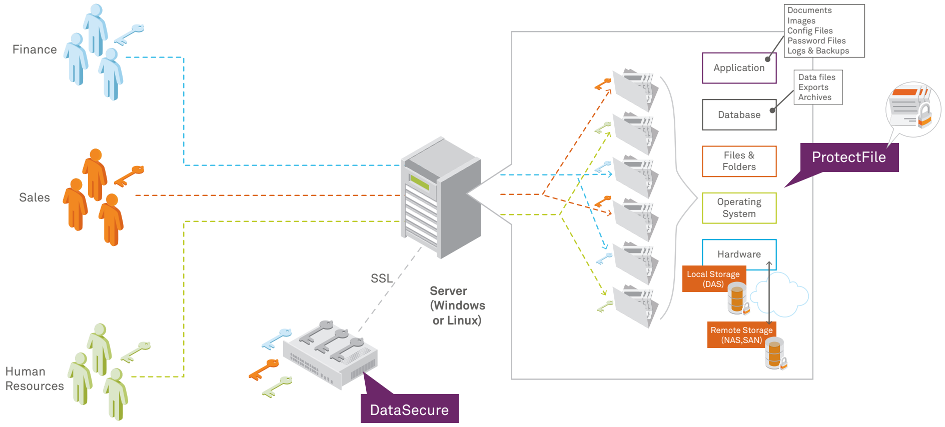
- Apache Hadoop
- Linux
    - Oracle
    - Red Hat Enterprise
    - Suse
    - Unbreakable Enterprise Kernel
- Microsoft Windows

Request Information

Contact us for more information and to learn how to get started with SafeNet ProtectFile today.

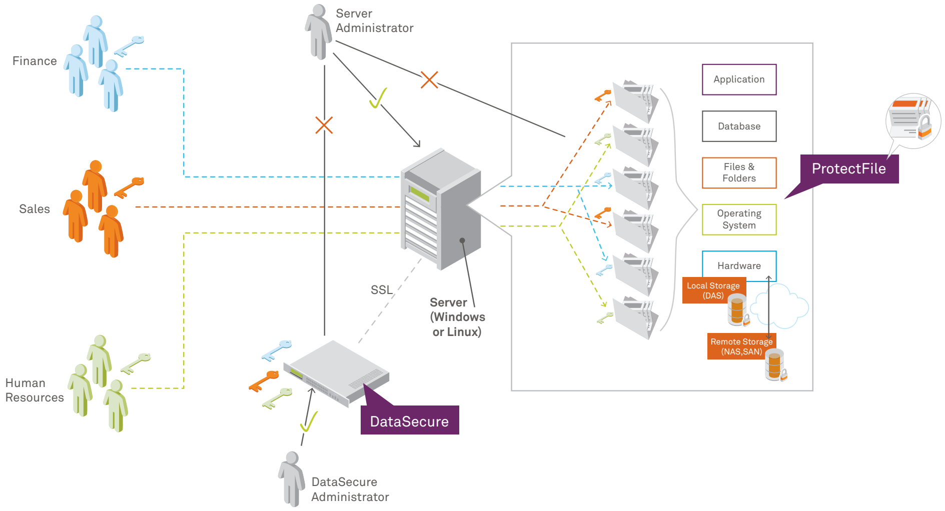
Segregate Sensitive Data on Shared Servers

In shared server environments, different departments and work groups may store sensitive data to the same server. With ProtectFile and DataSecure, administrators can easily isolate data by department on a server, and set policies to allow users to access segregated data only when they hold the proper encryption key.



Enable Strong Separation of Duties

The ability to separate duties based on business-need-to-know is fundamental to security best practices, and ensures regulatory compliance, while protecting sensitive data against internal threats. ProtectFile and DataSecure enable the implementation of granular access controls that decouple administrative duties from data and encryption key access. For example, server administrators can access files and folders containing sensitive data to perform physical infrastructure management tasks, such as the back-up and archiving of data, but they will not be able to access or view the data.



Improved Compliance

ProtectFile helps achieve compliance with a variety of regulations that require encryption of data including, but not limited to, credit card numbers for Payment Card Industry Data Security Standard (PCI DSS) compliance, Personally Identifiable Information (PII) to comply with state data breach and data privacy laws, and Electronic Patient Health Information (EPHI) in accordance with HIPAA.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/news-media