gemalto
security to be free

PRODUCT BRIEF

SafeNet ProtectFile

File System-Level Encryption

Today, perimeter-based security defenses cannot adequately secure the growing volume of sensitive data residing on servers in physical, virtualized, and public cloud storage environments. To be completely protected, organizations must employ a solution that attaches security to the data itself.

Due to its volume and relevance, high value data on enterprise servers is the most attractive and easily targeted. SafeNet ProtectFile provides transparent and automated file system-level encryption of server data at rest in the distributed enterprise. This includes data-centric protection of Direct Attached Storage (DAS), Storage Area Network (SAN), and Network Attached Storage (NAS) servers using CIFS/NFS file sharing protocols.

SafeNet ProtectFile also features granular access controls, centralized policy and key management, and comprehensive auditing capabilities. Once deployed, files containing sensitive data are rendered 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

SafeNet ProtectFile is deployed in tandem with SafeNet KeySecure, a FIPS 140-2 up to Level 3 enterprise key manager, for centralized key and policy management across multiple sites. The solution encrypts sensitivedata on servers, such as credit card numbers, personal information, logs, passwords, configurations, and more in a broadrange of flat files, including word processing documents, spreadsheets, images,designs, database files, exports, archives, and backups.

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

Highlights

Transparent, Strong, and Efficient Encryption

- Apply transparent and automated file system-level encryption in physical, virtual, and cloud environments
- Define and enforce granular access control policies
- Manage encryption keys centrally and securely in FIPS certified hardware

Privileged User Control

- Prevent rogue root administrators from impersonating other users and accessing protected data

Secure Data Archival and Destruction

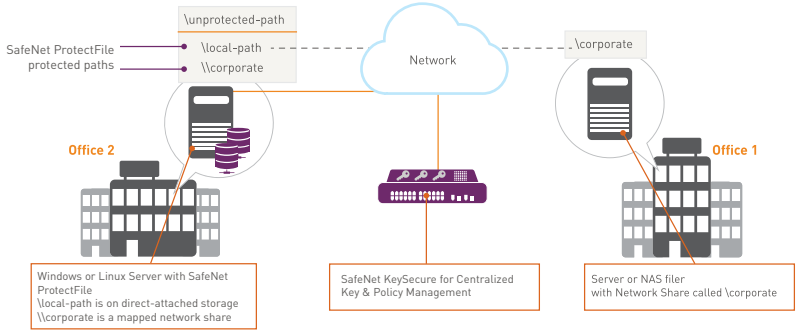
- Keep high value data encrypted and inaccessible to server administrators performing scheduled back-up and restore tasks
- Ensure all secured, sensitive data is rendered unreadable in the event destruction of data is required

Easy Implementation and Management

- Utilize remote, silent automation tools for quick and easy deployment in large and small environments
- Streamline administration and reduce overhead with centralized policy and key management
- Built-in, automated key rotation

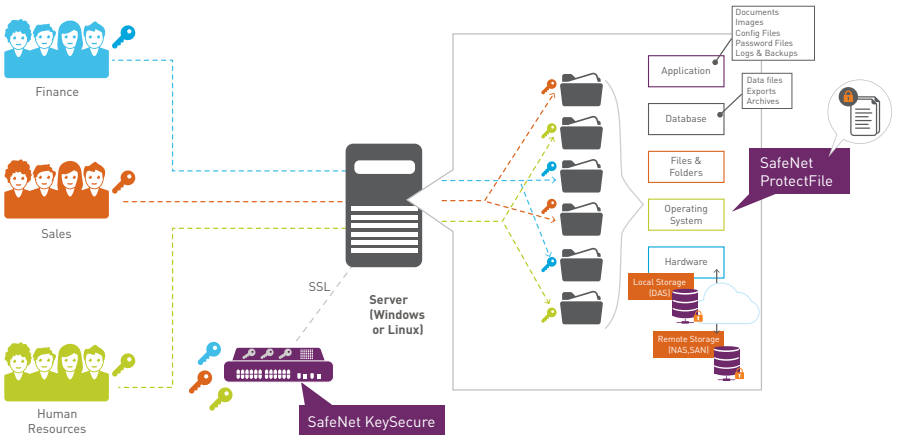
Achieve Compliance

- Ensure separation of duies
- Track and audit user access to protected data and keys



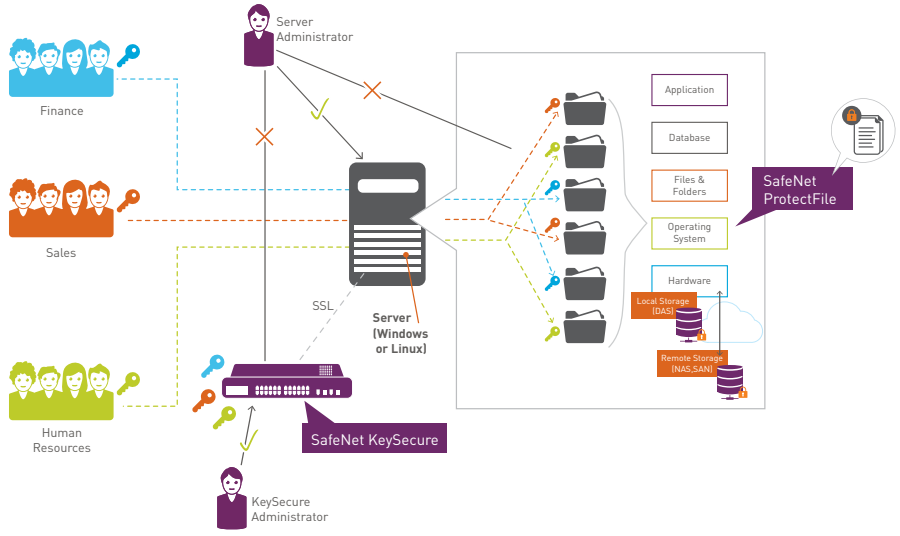
Segregate Sensitive Data on Shared Servers

In shared server environments, different departments and work groups may store sensitive data to the same server. With SafeNet ProtectFile and SafeNet KeySecure, 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. SafeNet ProtectFile and SafeNet KeySecure 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

SafeNet 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.

Request Information

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

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

- Linux: Oracle, Red Hat Enterprise Linux, SUSE
- Microsoft Windows
- Big Data: Apache Hadoop, IBM InfoSphere BigInsights
- Cloud: All public clouds, including AWS
- Cloud Management: Chef
- Databases: Cassandra, IBM DB2, Microsoft SQL Server, Microsoft SharePoint, mongoDB, Oracle
- Containers: Docker

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

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free