

# SafeNet ProtectFile for Dell EMC Storage

## Working Together to Secure Sensitive Data in Storage

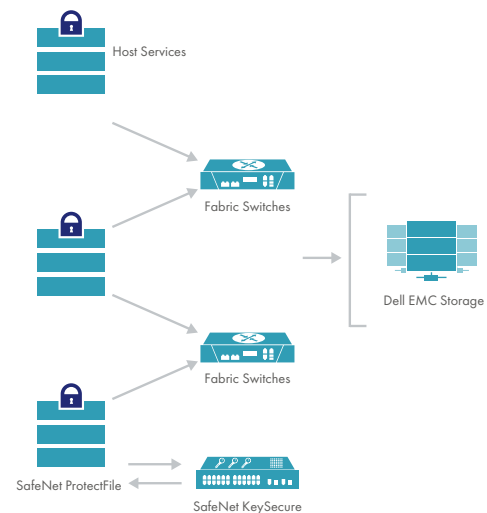


Secure sensitive data throughout its lifecycle wherever it resides with file system level encryption and granular access controls.

High value data on enterprise storage is among the easiest and most attractive targets for attackers. The volume is growing significantly within the enterprise – whether it is on physical, virtualized, or cloud-based storage environments. Perimeter security is neither infallible nor does it address internal risks to the organization. Only a data-centric approach to security will truly protect the sensitive data at the core of enterprise operations.

### Solution

Fortunately, customers can securely accommodate data storage's accelerating growth. Dell EMC Storage's high-performance, scalable platform integrates with Thales's SafeNet ProtectFile encryption to provide the data-centric security that will keep data safe in the event of a breach, misuse or hijacking of privileged accounts, physical server theft and other potential threats. Replicated and backed-up data will remain encrypted throughout its lifecycle; affording customers secure data protection across remote and Disaster Recovery sites.



### Dell EMC Storage

Dell EMC Storage optimizes data throughout its lifecycle via built-in intelligence that automatically places data on drives according to its level of use. Dell EMC Storage is a high-performance, efficient, and scalable platform based on a modular architecture that unifies block and file to help lower total cost of ownership. Real-time system information about each data block allows storage arrays to optimize placement, management, and protection throughout the lifecycle.

# SafeNet ProtectFile and SafeNet KeySecure

SafeNet ProtectFile automatically and transparently encrypts sensitive data-at-rest for SAN block storage. Customers can use this transparent encryption to secure such sensitive data as credit card numbers, personal information, logs, and more that reside in flat files such as word processing documents, spreadsheets, images, designs, SQL and NoSQL database files, exports, archives, Hadoop clusters, and backups.

SafeNet ProtectFile is deployed in tandem with SafeNet KeySecure – a FIPS 140-2 Level 1 or 3 validated hardware or software appliance for centralized encryption key and policy management. SafeNet KeySecure integrates with Dell EMC Storage via the Key Management Interoperability Protocol (KMIP) allowing customers to centralize the management of SafeNet encryption keys, as well as Authority Credentials from Dell EMC Storage self-encrypting Drives (SED) and other 3rd party encryption solutions.

## Benefits

### Transparent, Strong Encryption

- Apply transparent and automated encryption in physical, virtual, and cloud environments

### Apply Granular Access Controls

- Manage keys and policies centrally in FIPS-certified key manager
- Finely restrict data access by user, location, time of day, etc. to reduce internal risks in the organization

### Privileged User Controls

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

### Secure Archival of Data

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

### Secure Data Destruction

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

### Achieve Compliance

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

## How the Solution Works

### Segregate Sensitive Data in Shared Storage

In shared storage environments, different departments and business units may store data to the same server. With SafeNet ProtectFile and SafeNet KeySecure (or SafeNet Virtual KeySecure), administrators can easily isolate data by department on a server,

and set policies to allow users to access segregated data only when they have the proper permissions or according to a specific context (e.g time of day).

### Separate Duties Amongst Administrators

The ability to separate duties based on business-need-to-know is an important security best practice, ensures regulatory compliance, and secures data from internal threats. SafeNet ProtectFile with SafeNet KeySecure (or SafeNet Virtual KeySecure) offers policy based 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 infrastructure management tasks such as back-up and archiving without being able to access or view the data itself. Conversely, security administrators can manage encryption keys without ever having access to the storage environment. In addition, SafeNet KeySecure administrators can only manage the security policies and keys on the key manager.

### Make Compliance Easier

SafeNet ProtectFile helps organizations comply with a variety of regulations that require encryption including, but not limited to The European Union's General Data Protection Regulation (GDPR), PCI DSS state data breach and data privacy laws, Australia Privacy Amendment 2017, and HIPAA. SafeNet ProtectFile restricts data access to authorized users while SafeNet KeySecure's logs provide the oversight information key to demonstrate data control in accordance with regulatory mandates.

### Installation and Support

To ensure successful deployment, Thales's Professional Services team schedules on-site visits to install SafeNet KeySecure and get the customer up and running. In addition, Thales offers comprehensive on-going support packages in 1, 3, 4 and 5 year terms that cover mission critical business and operational issues. Throughout SafeNet KeySecure's lifecycle, Thales support is committed to ensuring customer satisfaction.

## Conclusion

Attaching security to data itself is critical to ensuring that it is safe in the event of a security breach. Dell EMC and Thales combine to offer organizations the ability to secure their sensitive data through encryption while preserving flexibility and control in their security and business operations. ProtectFile is part of the Thales's portfolio that bring data security at all levels of the enterprise data stack, including the application, database (column or file), file system, full disk (virtual machine), and network attached storage levels. For more, visit: <https://safenet.Thales.com/partners/dellemc/>