Gemalto SafeNet ProtectFile Solution for Dell Storage SC Series

Working Together to Secure Data-in-Flight

SAN block storage is an efficient, cost-effective way to scale enterprise storage as the need for additional capacity grows. Organizations need to secure data residing in these storage arrays against risks from insider and outsider threats. Using encryption to attach security directly on the data itself, secures it in SAN block storage environments and in all subsequent environments where data is replicated and backed up.

Transparent, Strong Encryption

- Apply transparent and automated encryption in physical, virtual, and cloud environments
- Apply granular access control policies
- Manage keys centrally and securely in FIPS-certified key manager

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

To be fully protected, customers can no longer count on perimeter-based security defenses alone. High value data on enterprise storage is among the easiest and most attractive targets for attackers. The volume of sensitive data is growing within the enterprise – whether it is on physical, virtualized, or cloud-based storage environments – and companies need to take a data-centric approach to security. The only way to truly secure the sensitive data at the core of enterprise operations, organizations must employ a solution that attaches security to the data itself.

Solution

Fortunately, customers can securely accommodate the accelerating growth in data storage. Dell Storage's high-performance, scalable platform integrates with Gemalto's SafeNet ProtectFile encryption to provide the data-centric security needed to render sensitive data useless in the event of a breach, misuse or hijacking of privileged accounts, physical theft of servers, and other potential threats. As data is replicated and backed-up, it will remain encrypted throughout its lifecycle; affording customers secure data protection across remote and Disaster Recovery sites.

Dell Storage

Dell Storage SC Series arrays,(including Dell Compellent solutions), optimizes data throughout its lifecycle via built-in intelligence that automatically places data on drives according to its level of use. The SC Series 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 SC Series 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, 2 or 3 validated hardware appliance for centralized encryption key and policy management. SafeNet KeySecure integrates with Dell 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 Storage Self-encrypting Drives (SED) and other 3rd party encryption solutions.

How the Solution Works

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

SafeNet ProtectFile Features

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, 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.

Separate Duties Amongst Administrators

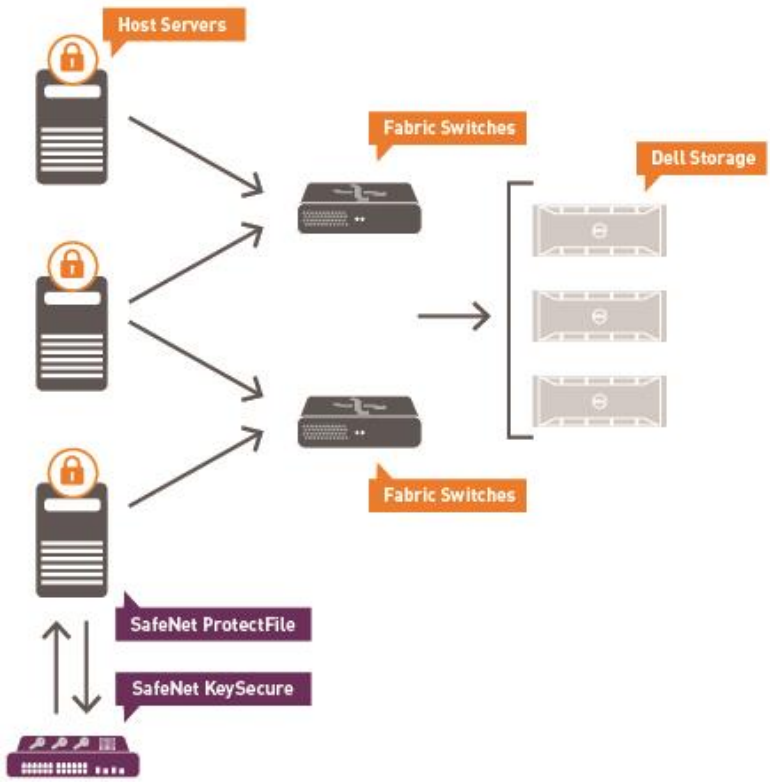
The ability to separate duties based on business-need-to-know is an important security best practice, and ensures regulatory compliance, while securing data from internal threats. SafeNet ProtectFile with SafeNet KeySecure enables the implementation of granular access controls that decouple administrative 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 back-up and archiving, but they will not be able to access or view the actual data itself, In addition, SafeNet KeySecure administrators can only manage the security policies and keys on the key manager.

Improve 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.

Installation and Support

To ensure successful deployment, Gemalto's Professional Services team schedules on-site visits to install SafeNet KeySecure and get the customer up and running. In addition, Gemalto 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, Gemalto 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 and Gemalto combine to offer organizations the ability to secure their sensitive data through encryption while preserving flexibility and control in their security and business operations. For more, visit: http://www.safenet-inc.com/partners/dell or contact: DellSales@safenet-inc.com.