

Dell Storage SC Series & Thales: Securing Data Using Transparent Encryption & Key Management



CipherTrust Transparent Encryption & Key Management helps customers secure their most valuable and sensitive asset – their data

- Structured and unstructured data security across physical, virtual, cloud, and big data environments
- Transparent- no application, database or infrastructure changes required
- Blind data to administrators through integrated OS privileged user access control
- Simplified key management by consolidating encryption key management & certificate storage
- FIPS 140 Level 2 and Level 3 certification
- Multi-tenant operations for compartmentalized management of data security policies, data encryption keys, and audit logs
- Centralized & Simplified data at rest security policies

The Challenge

Safeguarding more data, in more environments, against more threats

For IT and security teams today, adaptation is a key part of the job. Sensitive data continues to make it into a broader set of environments, including cloud deployments, big data platforms, virtualized systems, and more. The policies and regulatory mandates continue to grow more stringent. At the same time, these groups have to guard against more sophisticated cyber-attacks, and the continuous threats posed by malicious users with privileged access.

The Solution

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.

CipherTrust Transparent Encryption

With CipherTrust Transparent Encryption, organizations can establish strong controls around their sensitive data, and do so with maximum efficiency. CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control, and security intelligence to proactively meet compliance reporting requirements for structured databases and unstructured files. The solution can be deployed without any changes to applications, databases or infrastructure so security organizations can implement encryption with minimal disruption, effort, and cost.

CipherTrust Transparent Encryption delivers these key advantages:

- **Continuous protection.** This solution's protection does not end after the encryption key is applied. CipherTrust Transparent Encryption continues to enforce policies that protect against unauthorized access by users and processes, and it continues to log access.
- **Granular controls.** The product enforces granular, least-privileged user access policies that protect data from advanced persistent threat (APT) attacks and misuse by privileged users. Specific policies can be applied by user (including for administrators with root privileges), process, file type, time of day, and other parameters.
- **Security intelligence.** The solution provides detailed data event logs to satisfy compliance and forensic reporting, and enable additional data security analytics with popular security information and event management (SIEM) systems.
- **Flexible implementation.** CipherTrust Transparent Encryption is an agent that runs at the file system level or volume level on a server. The agent is available for a broad selection of Windows, Linux, and UNIX platforms, and can be used in physical, virtual, cloud, and big data environments—regardless of the underlying storage technology.

For central control, The CipherTrust Manager enables organizations to have a consistent and repeatable method for managing encryption, access policies, and security intelligence for all structured and unstructured data. Once CipherTrust Manager is in place, you can more quickly adapt to new security mandates, compliance requirements, and emerging threats.

Beyond Self Encrypting Drives

Self-encrypting drives (SED) is an excellent control for physical theft of the data. The Thales- Dell Storage Solution provides the additional security needed at the file system level or volume level on a server. This addresses the situation in the data center where devices such as servers are up and online at all times.

CipherTrust Key Management

Controlling and maintaining encryption keys is an essential part of any enterprise encryption and key management strategy. Silos of encryption without centralized key management can become a security administrator's nightmare, consuming time, budgets and putting data at risk of accidental compromise.

CipherTrust Key Management that supports the CipherTrust Transparent Encryption solution provides a robust, standards-based platform for managing encryption keys from disparate sources across the enterprise. It simplifies the management and administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services.

The Dell Technology Partner Program

Thales is a Dell Technology Partner and CipherTrust Transparent Encryption and Key Management is approved by Dell Storage to run on the Dell Storage SC series platforms specified in the above technical overview.

The Dell Technology Partner Program is a multi-tier program that includes ISVs, IHVs and Solution Providers. This global program helps partners build innovative and competitive business solutions using Dell Storage platforms. Program resources keep customer costs low and helps to sustain competitiveness.

The program has a structured and streamlined process that combines technology and business strategies with Dell Solution Center expertise to onboard and test partner products on Dell Storage platforms. This testing process helps ensure that products have met the technical requirements to perform well on Dell Storage platforms.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.