BROADCOM®

Product Brief

MegaRAID®
SafeStore™ Software

Key Features

- MegaRAID SafeStore software, together with self-encrypting drives (SEDs), secures a drive's data from unauthorized access or modification resulting from theft, loss, or repurposing of drives.
- Auto-Lock feature locks the drive and secures the data on the drive the moment a drive is removed from a system or a drive or system is stolen.
- Instant Secure Erase feature allows users to instantly and securely render data on SED drives unreadable, saving businesses time and money by simplifying decommissioning of drives and preserving hardware value for returns and repurposing.

Overview

Whether it is sensitive customer information, intellectual property, or proprietary data that helps a company reach its strategic objectives, a company's data may be its most valuable asset. If this data is misplaced or stolen, organizations run the risk of lost revenue, legal implications, and a tarnished reputation. The unfortunate truth is that an organization's data is becoming increasingly vulnerable as lost, accidentally exposed, or breached data is becoming more and more commonplace in today's environment. With data security risks on the rise, an influx of government mandates and regulations for securing data have been implemented and is becoming part of the corporate landscape for many. Eliminating exposure of private data is now simply viewed as a sound business practice.

Security for Data-at-Rest

To avoid the high costs associated with data exposures such as these, organizations must put in place a comprehensive security strategy. While each point in the storage infrastructure provides unique threat models, data-at-rest presents one of the highest security vulnerabilities. Data spends most of its life at rest on drives within the data center. As these drives will eventually leave the data center either for repair, retirement, relocation, or maintenance, it is at this time that drives — and the data contained on these drives — are most vulnerable to being lost or stolen.

The emergence of self-encrypting drives is timely in mitigating the security vulnerabilities of data-at-rest. Self-encrypting drives that adhere to the TCG (Trusted Computing Group) Enterprise Security Subsystem Class specification are National Security Agency qualified and provide unparalleled security with government-grade encryption. With SEDs, if a drive is removed from its storage system or the server it is housed in, the data on that drive is encrypted and useless to anyone who attempts to access it without the appropriate security authorization. Many safe harbor laws protect organizations that store data in compliance with security encryption requirements. In fact, in many cases, an organization will not have to notify a customer of lost data if that data was stored on secured self-encrypting drives.

Supported RAID Controllers	Electronic License	HW License Key
MegaRAID SAS 9361/9380 Series	LSI00268	LSI00287
MegaRAID Tri-Mode 9460/9480 Series	—	LSI00287
MegaRAID Tri-Mode 9560/9580 Series*	—	

* Included as a standard feature.

Simple and Secure SED Management

While the encryption capabilities of the drives are the primary level of security, management of the self-encrypting drives is critical to its execution. In fact, the security capabilities offered with drive-level encryption are only as good as the management tool used to implement and manage them.

As a leader in storage technologies, Broadcom® is pleased to offer SafeStore software, which provides local key management using the Auto Lock feature and also supports Instant Secure Erase for higher levels of data protection over traditional drive retirement methods. With SafeStore software, businesses have the assurance that the highest level of security is placed on their data, while preserving system performance and ease-of-use.

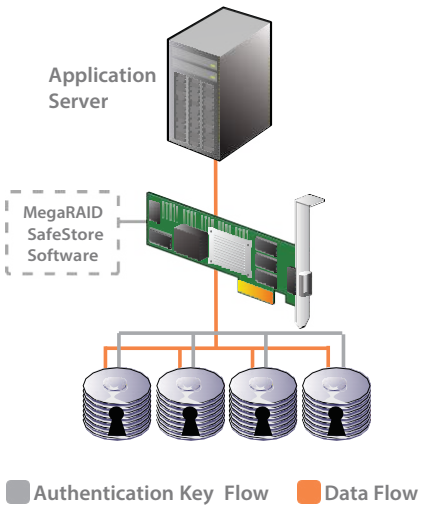
Auto Lock with Local Key Management

Auto Lock with Local Key Management locks the SED using an authentication key. When secured in this manner, the drive's data encryption key is locked whenever the drive is powered down. In other words, the moment the SED is switched off or unplugged, it automatically locks down the drive's data. When the drive is powered back on, it requires authentication before being able to unlock its encryption key and read any data on the drive. This protects against any type of insider or external theft of drives or systems.

Instant Secure Erase

Instant Secure Erase provides instant data protection via cryptographic erase. Whether the drive is 73GB or 1TB, this feature will delete the existing data encryption key and regenerate a new data encryption key in seconds, enabling drives to be returned, retired, sold or reused securely. If you decide to use Instant Secure Erase only (without Auto Lock), you will not be required to maintain authentication keys or passwords in order to access the drive's data. The SED will automatically encrypt the data being written to the drive and decrypt data being read from it. When it is time to retire or repurpose the drive, the owner simply sends a command to the drive to perform the cryptographic erase. This command replaces the encryption key inside the encrypted drive, making it impossible to ever decrypt the data. Using Instant Secure Erase, businesses can save time and money by simplifying decommissioning of drives and preserving hardware value for returns and repurposing.

Figure 1: MegaRAID Controller



Drive Retirement Options

Drive Retirement Option	Advantages	Disadvantages
Destruction	• Effective way to destroy the drive if done correctly.	• Will not allow for reuse of the drive. • Can be costly when considering destruction, hauling and dumping costs. • Time consuming. • Not environmentally friendly.
Degaussing	• Effective way to destroy the drive if done correctly.	• Machines needed for degaussing are very expensive. • Short duty cycle make it unsuitable for deleting large number of drives in short time. • Will typically not allow for reuse of drives. • Not environmentally friendly.
Overwriting	• Minimal upfront cost for overwriting software • Allows for reuse of the drive. • Effective if drive is overwritten at least three times prior to disposal or reuse.	• Extremely time-consuming. • Tying up system resources with overwriting cycles is likely to off-set cost savings. • If the drive is being retired due to an error on the drive, this eror may prevent completion of the overwriting process.
Instant Secure Erase	• Saves time and money as compared to other drive retirement alternatives. • Allows for reuse of the drive. • Instantaneously makes data unreadable. • Allows administrators to render drive unreadable remotely.	• Small, incremental cost for SED over non-SED hard drives.

BROADCOM®
connecting everything®

For more product information: broadcom.com

MR-SafeStoreSW-PB100 March 17, 2020