



EXECUTIVE SUMMARY

As a small or medium business (SMB), you are facing many of the same security challenges that large corporations face. In fact, regardless of your company's size, it is required to adhere to new laws mandating better protection for sensitive or confidential data. But, with small security budgets, a shortage of dedicated IT resources, and limited experience with encryption technology, SMBs are less likely to take the necessary steps to protect against data breaches.

These obstacles may have prevented you from adopting or implementing new security technologies in the past. However, recent developments in disk encryption have made comprehensive data security both affordable and easy. The combination of Seagate Secure™ Self-Encrypting Drives (SEDs) and LSI SafeStore Encryption Services removes the complexity and high cost of obtaining and managing encryption technology, which virtually eliminates the risk of damaging data breaches.

Seagate® Self-Encrypting Drives and LSI SafeStore™: Simplifying Encryption and Data Security for Small and Medium Businesses

Why is now a good time to invest in Seagate Secure™ SEDs and LSI SafeStore?

You need to comply

Large corporations are not the only businesses subject to regulatory compliance requirements related to security practices. As an SMB, you are faced with the same compliance requirements as Fortune 500 companies, but with additional obstacles in actually adhering to them; smaller budgets, shortage of dedicated IT staff, and a limited knowledge of the countless security solutions.


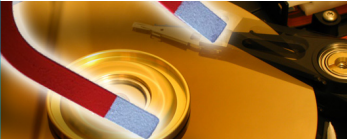

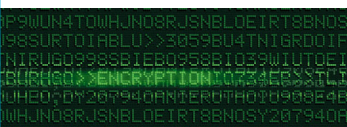
Studies have shown that the majority of SMBs are aware of the security threats on their business, but have failed to adequately protect their data by strengthening their security infrastructure. Perhaps you feel that because you are an SMB, your data is undesirable to thieves. Unfortunately, nothing is further from the truth. Criminals often target SMBs with 'smash and grab' theft because they are easier to penetrate than large businesses.

Regardless of your current outlook on data security, new compliance requirements, the rise in data breaches and new security technologies will drive you to strengthen your security infrastructure sooner than later. Choosing the right solution today will protect your business from costly breaches that can seriously wound your bottom line and reputation.

It will save you time and money with drive retirement and disposal

Since the vast majority of retired drives contain sensitive data, you should either remove the data or completely destroy the drive before it leaves the organization for repair, reuse, or retirement. But many organizations either fail to understand the risks of leaving data on drives and take no action to remove it, or mistakenly believe the data has been safely deleted when in fact it can still be recovered.

There are currently four approaches to retiring and disposing of hard drives. Each method has various advantages and disadvantages. The following sections detail the pros and cons of each approach.

Drive Retirement Options	Advantages	Disadvantages
Destruction 	<ul style="list-style-type: none"> • Effective way to destroy the drive if done correctly 	<ul style="list-style-type: none"> • Will not allow for reuse of the drive • Can be costly when considering destruction, hauling and dumping costs. • Time consuming • Not environmentally friendly
Degaussing 	<ul style="list-style-type: none"> • Effective way to destroy the drive if done correctly 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 error may prevent completion of the overwriting process.
Instant Secure Erase 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Small, incremental cost for SED over non-SED hard drives

Destruction: Physical destruction is typically done by shredding the entire drive or the drive's platters. At a minimum, the platters must be badly warped or distorted, rendering the drive or any of its components inoperable. This can generally be achieved by drilling the drive in several locations perpendicular to the platters and penetrating completely through from top to bottom. Hammering or crushing is equally effective but more labor intensive. Simply destroying the logic section of the drive without damaging the platters is insufficient and not recommended.

Degaussing: Degaussing to erase the magnetic media on the drive requires specialized equipment designed and approved for the type of media being purged. Industrial degaussers rated for hard disks are very expensive. Further, their duty cycle is relatively short, making them questionable for deleting large numbers of drives in a short time. Drives that are degaussed will generally be unusable.

Overwriting: Overwriting a hard drive requires a software program that writes a combination of 0s and 1s over each location on the hard drive multiple times. This process obscures the previous information under multiple layers of magnetic flux, rendering the data unreadable. According to the Department of Defense, functional drives should be overwritten three times prior to disposal or reuse.

Overwriting software costs between \$50 for a single license up to \$2000 for professional versions. This is a less expensive alternative to degaussing or destroying a hard drive. Plus, overwriting does not destroy the drive, so the device may be reused.

However, overwriting is very time-intensive and may not even work if the drive has an error. Because overwriting tools repeatedly write data to every track, erasing a disk in this manner can take hours to days depending on the number of passes performed, the size of the drive and the speed of the system. In the end, the amount of time that overwriting takes may offset the cost savings for many organizations.

Instant Secure Erase : Instant Secure Erase on Self-Encrypting Drives (SEDs) is the newest method of rendering hard drive data unreadable via a cryptographic erase of the data encryption key. This method is very effective, instant and simple to administer. It works by first encrypting all data as it is written to disk. The only way to read or obtain data protected in this manner is to use a valid encryption key. Instant Secure Erase will render all data on the SED unreadable when the encryption key is destroyed.

There are many advantages to using Instant Secure Erase for retiring or reusing hard drives as compared to the alternatives. First, it is instantaneous. A command can be issued by an administrator to instantly destroy the encryption key, making all the data immediately unrecoverable. Also, Instant Secure Erase can be performed remotely*. There is no need to gather retired equipment into a secure location while they await erasure.

Instant Secure Erase with SEDs is also a very cost-effective solution. It allows for reuse of drives, eliminates the expense and time required to destroy, degauss, or overwrite, and requires only an incremental cost over non-SED hard drives to purchase SEDs. This marginal cost of SEDs more than compensates for the time spent retiring drives and the cost of a potential data breach.

It's one of the easiest and most cost-effective security measure you can implement

There are many different types of encryption to choose from; host-based, appliance-based and SED-based. All of them have their benefits and drawbacks, but encryption using SEDs is an easy, secure, and affordable method of protecting your critical data.

Host-based Software Encryption : Host-based encryption is implemented using software. In some cases, your business may already be using software that has encryption capabilities. The benefits of software encryption are that it is affordable and may already be included in software that you use.

However, there are some major drawbacks to host-based encryption. The most obvious is related to performance. Because host-based encryption uses the host CPU, processor cycles are taken away from other host-based applications. This puts a major drain on system performance, which leads businesses to encrypt only a small percentage of sensitive data. This requires data classification which is time-consuming and error-prone. What's more, it leaves data unencrypted which makes businesses more vulnerable to data theft or software attacks.

Host-based encryption also raises concerns for manageability. SMBs that do not have dedicated security or IT resources will struggle if there are large amounts of data to encrypt. Since host-based solutions are system-dependent, they will require regular updates. For example, if your operating system is patched, the encryption software may need to be updated as well. If there are not some rigorous maintenance practices in place, your encrypted data and keys are vulnerable to unauthorized access.

Significant impact on system performance paired with complex implementation and management make host-based encryption an unattractive option for SMBs that are serious about protecting their data with their limited resources.

*Remote management is a value-add service of MegaRAID Storage Manager™ (MSM)

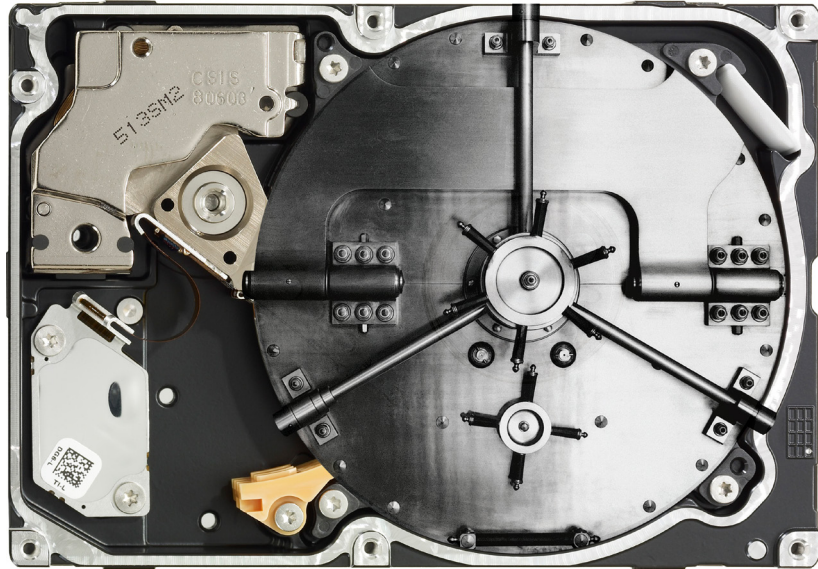
“Self-Encrypting Drives are one of the easiest, most cost-effective security measures companies can implement.

The use of SEDs provides businesses with complete data-at-rest protection against information breaches that can occur in drives and systems that have been repurposed, decommissioned, disposed of, sent for repair, misplaced or stolen. Because all disk media eventually leaves a company's control, the use of SEDs ensures that data is protected at these critical stages of a system's life cycle.”

Eric Ouellet

Vice President, Gartner

The Seagate SED solutions are based on TCG specifications to enable integrated encryption and access control within the protected hardware of the drive.



Appliance-based : Appliance-based encryption is accomplished by inserting an encryption appliance into your existing network or infrastructure. Appliance-based encryption overcomes many of the shortcomings of host-based encryption, but still has many drawbacks when compared to using SEDs for encryption.

While host-based encryption uses CPU cycles to secure your data, appliance-based solutions use microprocessor-based hardware systems fully dedicated to encryption. This means that any performance degradations you may see with host-based solutions will be unrecognizable with appliance-based solutions. Another benefit of an encryption appliance is its ability to protect data in transit. This means that the data is encrypted from the appliance to the destination storage device.

However, there are some drawbacks to appliance-based encryption. The most obvious is the cost associated with it. Encryption appliances can cost upwards of tens of thousands of dollars. And as your storage requirements grow, so does your need for additional encryption appliances. Adding more encryption appliances makes your ability to manage encryption of the data increasingly difficult. The high price tag combined with limited scalability make appliance-based solutions impractical for SMBs that have smaller budgets to implement a long-term security plan.

SED-based Encryption : Encryption using SEDs has revolutionized security by encrypting every piece of data on the drive itself. There is no longer the need to spend valuable time and resources on data classification because it is all encrypted. Unlike other encryption methods, SEDs offer affordable data security with no impact on performance. The SED's hardware encryption engine, which resides in the drive, matches the drive port's maximum speed and encrypts all data with no performance degradation. This performance scales linearly and automatically, with each drive added to the system.

And, while appliance-based encryption requires an additional investment each time your storage grows, SEDs can be added with only a small, incremental cost over the hard drives that you are already buying for additional storage. There is no other expense to incur.

Some other benefits of SED-based encryption are manageability and interoperability. SED encryption is automatic and transparent, which eliminates many of the costs associated with other forms of encryption including complicated installations and changes to the system, software,

or applications. And for additional ease-of-use and familiarity, SEDs appear just like any other hard drive when viewed with management software such as LSI SafeStore encryption services.

The price is right

Investing in SEDs can save your business up to millions of dollars by protecting against a data breach. And with incremental solution costs approximately 10% higher than comparable non-SED hard drive options, even one-man IT operations can afford this powerful security technology.

With host-based encryption options, you will incur costs for the additional storage required to hold uncompressed data and compensate for diminishing performance. Similarly, appliance-based encryption can be very expensive. As your storage requirements grow, so does your need for additional encryption appliances to support your growing infrastructure.

In addition to the upfront software and hardware costs of host- and appliance-based encryption, there are also the overhead costs associated with classifying, monitoring and maintaining the data. Since SEDs encrypt every bit of data on the drive there is no additional expense required for classification, maintenance, etc. Also, SEDs make drive retirement and disposal easy by eliminating the need for manual data destruction processes which can be expensive, complex and prone to error. In the end, the incremental cost of SEDs is offset by the savings you realize by avoiding these costly alternatives.

How do Seagate Secure™ SEDs and LSI SafeStore™ work?

The Seagate SED solutions are based on TCG specifications to enable integrated encryption and access control within the protected hardware of the drive. SEDs provide the industry's premier solution for full disk encryption, protecting every bit of data on the drive when systems or drives are lost or stolen, or when businesses need to retire drives or send them for repair.

Seagate Secure™ SEDs can be used for either or both of the following methods of data protection.

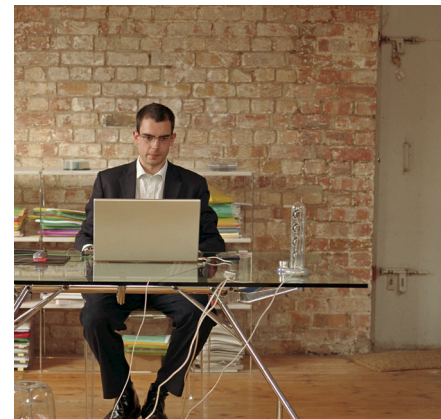
Auto Lock with Local Key Management

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.

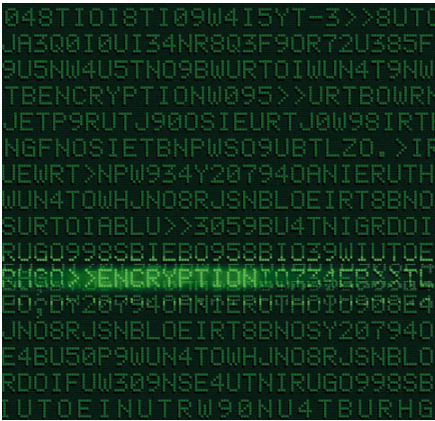
When the drive is powered back on, it requires authentication before being able to unlock its encryption key and read any data on the drive. This protects against any type of insider or external theft of drives or systems.

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 less than a second, 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.



Because SEDs require only a small incremental cost (~10%) over non-SED hard drives, even one-man IT operations can afford this powerful security technology.



LSI SafeStore Encryption Services provide local key management using the Auto Lock feature and also support Instant Secure Erase for higher levels of data protection over traditional methods.

Until now, there has not been a truly secure or cost-effective method to protect data on a retired drive. In fact, a study conducted by IBM found that approximately 90% of drives returned for warranty repair contain readable data. Using Instant Secure Erase, businesses can save time and money by simplifying decommissioning of drives and preserving hardware value for returns and repurposing.

LSI SafeStore Encryption Services

LSI SafeStore Encryption Services provide local key management using the Auto Lock feature and also support Instant Secure Erase for higher levels of data protection over traditional methods. While the encryption capabilities of the SEDs are the primary level of security, management of them is critical to their execution. With SafeStore, SMBs have the assurance that the highest level of security is placed on their data, while preserving system performance and ease-of-use.

This sounds great, but...

How will this change my IT infrastructure?

The addition of SEDs will have very little impact on your existing IT infrastructure. A major advantage of SEDs is their ability to automatically and transparently encrypt data, without costly changes to your existing systems, software or applications. And for added ease-of use, management software like LSI SafeStore allows you to view, configure and manage SEDs just like a normal hard drive.

Also, for maximum utilization of drive inventory, businesses may continue to use their existing hard drives for data that they do not deem 'sensitive'. And when it becomes necessary to secure data residing on traditional hard drive, the data can be simply migrated to an SED. With the ability to support SEDs and traditional HDDs in the same system, LSI MegaRAID® controllers with SafeStore encryption services allow SMBs to upgrade their infrastructure at their own pace.

Will encryption degrade application performance?

No. Encryption using SEDs helps avoid the performance pitfalls of other types of encryption.

Even though encryption appliances tend to be very fast, as systems grow and more data is encrypted and decrypted, the appliances can become a performance bottleneck. This is because all the encryption/decryption is occurring on the appliance.

Alternatively, SEDs have an encryption engine that resides on the drive itself. That means CPU cycles from the host are not used and the transfer of I/Os can occur without interruption. Also, since the encryption/decryption is happening on each drive independently, your system will not suffer from performance bottlenecks as your storage requirements grow.

What if I lose the authentication key?**

If you forget the authentication key or lose the key when using Auto Lock, the data is also lost. For this reason, it is important that you store the key in multiple secure locations and with multiple trusted people. Note: To take advantage of Instant Secure Erase, there are no authentication keys required. The authentication keys are only needed for the Auto Lock feature.

Can I afford it?

Purchasing SEDs requires only an incremental (~10%) investment over traditional hard drives. So, when you are ready to upgrade or retire your existing drives, you can invest in SEDs for a cost-effective security solution.

**Within MSM, the authentication key is referred to as the security key



Will my encryption environment scale?

Absolutely. Unlike other encryption methods, SED performance scales linearly and automatically. Because each SED contains its own encryption engine, there is no need to worry about balancing encryption workloads when adding more drives to the system. And unlike other methods of encryption, there is no additional hardware to invest in when adding more drives.

Conclusion

There are increasingly more reasons for small and medium businesses to want to and need to encrypt their sensitive data. In the past, there have been countless barriers to make data encryption a reality though. The options available to SMBs were too expensive, too resource-consuming, too slow or all of the above. But, with the introduction of Seagate Secure™ SEDs and LSI SafeStore, your business can work towards a comprehensive security plan that is both affordable and easy to implement.

SED performance scales linearly and automatically, so there is no need to worry about balancing encryption workloads when adding more drives to the system.

For more information and sales office locations, please visit the LSI web sites at
lsi.com lsi.com/contacts

LSI and LSI and Design logo are trademarks or registered trademarks of LSI Corporation. All other brand and product names may be trademarks of their respective companies.

LSI Corporation reserves the right to make changes to any products and services herein at any time without notice. LSI does not assume any responsibility or liability arising out of the application or use of any product or service described herein, except as expressly agreed to in writing by LSI; nor does the purchase, lease, or use of a product or service from LSI convey a license under any patent rights, copyrights, trademark rights, or any other of the intellectual property rights of LSI or of third parties.

Copyright ©2009 by LSI Corporation. All rights reserved.
September 2009

