Technology Paper

How to Make Drive Retirement Safe, Fast and Easy

Introduction

With hard disk drives (HDDs) and solid state drives (SSDs) storing vast quantities of highly sensitive data, data centers must find a secure way to retire these drives at the end of their life. However, the most commonly used methods, overwriting and destroying the drive (either in-house or through the use of a third-party service), are costly, time consuming and frequently fail to protect sensitive data completely. This paper describes how Self-Encrypting Drive (SED) technology with Seagate Instant Secure Erase (ISE) capabilities can dramatically reduce the time, cost and hassle of retiring hard drives while maintaining the ultimate in data security.

The Dilemma: How to Retire Drives While Securing Data

HDD and SSD products typically have a three- to five-year lifespan, not because they fail, but because technological advances simply make them outdated. This leaves organizations with a dilemma. How can they safely, quickly and cost-effectively retire enterprise drives while protecting the critical data they contain?

Data protection is no trivial matter. Industry analysts estimate that 80% of corporate laptop and desktop PCs—and even higher percentages of enterprise servers—contain sensitive personal and financial information or intellectual property that must be secured. Regulations such as HIPAA, Gramm-Leach-Bliley and Sarbanes-Oxley all require organizations to protect the privacy of this data. Many states even have data breach laws, such as California's SB-1386 Security Breach Information Act, that require all potential victims be notified when there is reason to believe their data could have been compromised. As a result, these regulations render security breaches extremely expensive. The overall cost of a security breach per compromised record ranges from US$50 to US$300, depending on the sensitivity of the data, and includes discovery and notification, lost productivity, lost customers, regulatory fines and remediation. In short, it is imperative that the data on retired drives stays out of the wrong hands.

How to Make Drive Retirement Safe, Fast and Easy

Current Processes Take Too Long, Cost Too Much and Don't Always Protect Data

Organizations that take data security seriously expend considerable time, effort and money disposing of drives in a secure manner. When organizations retire drives, they typically overwrite the drives and/or physically destroy them. Data centers often outsource the task of destroying the drive to an off-site third party. Alternatively, IT organizations repurpose their drives by overwriting the drive in the data center and shipping it to another data center or location, a costly and time-consuming process that is also prone to failure. For more information on the advantages and disadvantages of existing drive retirement methods, refer to Appendix A.

SEDs With Seagate Instant Secure Erase—Simplify and Reduce Costs for Drive Retirement

SEDs with Seagate Instant Secure Erase capability address the disadvantages of existing methods of decommissioning hard drives by providing a hassle-free, fast, cost-effective and secure alternative.

SEDs perform full disk encryption. The most secure of these solutions use AES-256 or AES-128 encryption algorithms, and the United States National Institute of Standards and Technology (NIST) certifies these encryption algorithms to meet the standards for use in government transactions for Level 2-type data. Data enters the drive and is encrypted before it is written to the disk using a dedicated ASIC chip. The data encryption key is stored in a secure, non-accessible area within the drive. When a Read is performed, the encrypted data on the disk is decrypted as it leaves the drive. The SED is always on—that is, it is constantly encrypting and the encryption cannot be turned off. During normal operation, the encryption operations on an SED are completely transparent. SED drives appear the same as non-encrypting drives without any impact on the performance of the system.

Retiring an SED With Seagate Instant Secure Erase

Seagate Secure™ SEDs generate their own encryption key using a methodology validated by NIST as being safe. When the time comes to retire the drive, an administrator simply changes the data encryption key. And without the correct data encryption key, the data on the drive is instantly and automatically unreadable and the drive is available to reformat safely.

When compared to other methods, Seagate ISE saves hours of handling for every drive. A 3TB drive can be cryptographically erased in less than one second as opposed to 39 hours to overwrite the drive three times. Seagate ISE mitigates all the costs of sanitizing by destruction or overwriting. Data centers no longer need to overwrite the drive, pay for machines to destroy the drive, or hire third party to destroy and dispose of the drive. Because the hard drive is not destroyed, cryptographically sanitized drives can be safely reissued within the organization, sold or donated for reuse.

Conclusion

Traditional methods of retiring and repurposing drives are time-consuming, costly and—despite a data center's best efforts—may fail to entirely mitigate the risk of a data security breach SED technology with Seagate Instant Secure Erase provides the optimum secure solution. By using a drive that automatically encrypts data as it is written to the drive, data centers that wish to retire their drives can literally throw away the encryption key. The data remaining on the drive is no longer accessible—by anyone. Data centers save considerable time, effort and money, and can literally dispose of the drives or reuse them without ever having to worry about the safekeeping of their data.

How to Make Drive Retirement Safe, Fast and Easy

Appendix A: Advantages and Disadvantages of Existing Drive Retirement Methods

The two most common methods of retiring drives today are:

- Overwriting drives
- Physically destroying drives

This section discusses the pros and cons of each approach.

Overwriting Drives

Regardless of whether they plan to destroy or repurpose the drive, the data center usually overwrites the data. Overwriting prevents data from being compromised en route to a destruction facility and ensures that new users of repurposed drives cannot access any of the data.

To overwrite the drive, the data center uses a software program to write a combination of 0s and 1s over each location on the hard drive, replacing useful data with garbage data that obscures the previous data. Depending on the value of the data and/or any industry governing standards, multiple overwrites may be required.

By following data overwrite standards, organizations can ensure that their data cannot be recovered. Overwriting standards include the United States Department of Defense (DoD) 5220.22, which specifies that functional drives be overwritten three times prior to disposal or reuse, and the United States National Institute of Standards and Technology (NIST) 800-88, which renders hard drives unrecoverable after a single wiping pass.

Advantages of Drive Overwrite

Because overwriting does not destroy the hard drive, the device can be repurposed. This can save a company several hundred dollars per drive, depending on the remaining life of the drive and the cost of a new one. If the drive is destined for physical destruction, overwriting prevents the data from falling into the wrong hands.

Disadvantages of Drive Overwrite

Overwriting the drive, however, is time consuming, prone to failure and costly.

Time-consuming—In today's data center, hard drives have very large capacities. Three terabytes are common, with 4TB and even 5TB drives on the horizon. With such large capacities, it can take hours or even days to complete the overwrite operation, depending on the numberof passes performed, the size of the drive and the speed of the system. For example, it takes 13 hours to reformat/overwrite a 3TB drive one time. Typically, the overwrite process is performed three times if the drive will be repurposed–for a total of 39 hours per drive. As drives become larger, the necessary overwrite time will only increase.

The operation can fail—A drive may be a candidate for decommissioning because of data errors or some other failure, and these problems can cause the overwrite to either time out or fail outright. A servo error may prevent the drive from being able to locate some data and/or overwrite it. For example, one customer found that the overwrite process frequently failed. If the operation hung after an hour or two, they would restart the process. If it hung after 8 to 10 hours, they would abort the process and destroy the drive on premises, which increased costs and presented security risks. For this reason, data center staff had to stay nearby and babysit the process to determine when the process failed, increasing the labor costs associated with the overwrite process.

Costs—In addition to costs associated with data center staff babysitting overwrite processes, the cost of software programs to sanitize hard drives can vary widely, ranging from freeware, to US$70 for a one-user license, to as much as US$4,000[1] for a 1000-user license.

Physically Destroying Drives

Organizations commonly destroy drives they do not repurpose. Often drives are drilled through from top-to-bottom, shredded, hammered or crushed. Organizations have a choice of destroying the drives themselves, having an outside company perform the destruction in the data center or sending the drive to a third-party firm for off-site destruction.

1 Sources—Survey of solutions from Multi-wipe (www.multiwipe.com), iolo Technologies DataScrubber (www.iolo.com), Lsoft Technologies Active@KillDisk (www.killdisk.com), White Canyon Software WipeDrive (www.whitecanyon.com), Jetico BCWipe (www.jetico.com), Kroll Ontrack Eraser (www.krollontrack.com).

How to Make Drive Retirement Safe, Fast and Easy

In-House Destruction

When a drive cannot be overwritten, some data centers will not let the drive out of the data center for security reasons. Destroying the drive oneself offers the highest level of security since no outsiders enter the data center. Disadvantages include time, effort and money. The cost of the machinery to perform the destruction can be steep—from US$950 for a small manual destroyer to US$45,000 for a unit the size of a commercial copier.[2] The IT staff must take the time to destroy the drives. Because physically shredding the drives is environmentally hazardous, the IT staff must carefully coordinate hauling and dumping

Outsourced, On-Site Destruction

Outside companies can come into data centers and perform the destruction on-site to ensure that an unsecured drive never leaves the site. This option eliminates the risk of losing a drive. It is also convenient, since the IT staff does not have to take the time to physically destroy the drive and haul it away. The downside is that this option is costly. Third parties impose a truck charge in addition to the standard drive destruction fee. It also presents a security risk because outsiders enter their secured areas.

Outsourced, Off-Site Destruction

Most often, companies use an outside firm to destroy the overwritten drives off-site. With this option, no outside firms enter the data center and the outside firm handles the waste disposal. This option can be costly, depending on quantity, and it does not entirely eliminate security risks—particularly if the data center has not properly overwritten the drives. Data centers must therefore ensure that the service they hire has in place and adequately follows best practices in drive disposal. The outsourced company must establish an unbroken chain of custody—some companies provide consoles in which customers lock their drives, and use those consoles to transport the drives to waiting trucks until they are shredded. The outsourced company then issues a certificate of destruction to verify that the process has been followed from beginning to end.

2 Sources—Data Devices International (www.datadev.com)

www.seagate.com

Seagate Secure®

AMERICAS Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, 408-658-1000
ASIA/PACIFIC Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00