WINMAGIC DATA SECURITY | Knowing You're Protected

White Paper

Reduce the total cost of ownership of laptops and desktops

Effective end-of-life drive sanitization and disposal

Jan/2011

200 Matheson Blvd. West, Suite 201 | Mississauga, ON | L5R 3L7
Tel: (905) 502-7000 |Fax: (905) 502-7001 | info@WinMagic.com | www.winmagic.com

Table of Contents

Synopsis

Full-disk encryption (FDE), used to protect sensitive data-at-rest residing on laptops or desktops, can be leveraged for end-of–life decommissioning of hard drives. FIPS and Common Criteria certified AES algorithms ensure that hard drives are fully encrypted, with the exception of the Master Boot Record (MBR). As a result, the data residing on the drives is not accessible to unauthorized users because it is entirely protected.

Encryption professionals put forward the proposition that destroying or overwriting the encryption key on fully encrypted hard drives is a plausible and real way of sanitizing[1] them. This method is commonly referred to in the industry as "crypto erase". This whitepaper compares the traditional sanitization methods (overwrite, degauss, and destroy), outlined in National Institute of Standards and Technology (NIST) SP 800-88, to the crypto erase method.

Regulatory agencies and encryption professionals are currently studying crypto erase as a potential sanitization method of future updates to publications like NIST SP 800-88.

[1] The term "sanitization" is used in this publication as it is defined in NIST Special Publication 800-88: "Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs." Sanitization methods include purging (overwriting and degaussing) and destroying.

Overview

In 2006, SANS Institute published an article entitled *The Ten Most Important Security Trends of the Coming Year*, which listed two of the following top three security trends: laptop encryption will be mandatory and preinstalled on new equipment destined to house sensitive data; and privacy protection legislation will become more stringent. And all for good reason, according to the Privacy Rights Clearinghouse (PRC), in 2010, there was a 240%[i] increase in reported data breaches from the previous year.

In response to the increasing number of data breaches and tighter privacy regulations, organizations should examine the lifecycle of their notebooks. First, notebooks / desktops are procured and given to an organization's IT department in order for any data to be removed from the hard drive, re-imaged for the respective organization, and then configured and customized for the intended recipient or employee within the same organization. Today, these same endpoint devices are being encrypted sector-by-sector using software full-disk encryption. Once the process is finished, they are delivered to the end users. As the user(s) performs their assigned tasks, data is written to the notebook / desktop, but never in clear text because the disk is encrypted. Eventually, the user(s) will either leave the organization or will be provided a new notebook / desktop, at which time the old one will need to either be re-purposed or decommissioned.

Because notebooks / desktops are encrypted before data is written to the drive, the data sanitization process is simplified; no clear text is available for unauthorized users to read throughout the drive's lifetime, even while it is awaiting sanitization or destruction. Additionally beneficial is the exception clause in some privacy and security legislation, such as the HITECH Act[ii], CS 1386, GLBA, etc., which does not require organizations to publicize the loss of sensitive data if it is encrypted.

This article examines how organizations can get an even better ROI on their FDE solution by comparing the traditional sanitization methods to the alternative method generally referred to in the industry as crypto erase. Crypto erase for software and hardware based encryption, enables administrators to restore a hard disk to factory standards in less than one second by overwriting the media's encryption key (MEK) / data encryption key (DEK), hence cryptographically shredding the hard drive.

Problem

Between 2000 and 2002, two Massachusetts Institute of Technology (MIT) students, Simson L. Garfinkel and Abhi Shelat, acquired 158 hard drives from a second hand market[iii] from which they were able to retrieve thousands of credit card numbers and private personal information. In order to properly safeguard their data, NIST (SP 800-88) recommends that organizations apply one or a combination of the following three traditional media sanitization methods: overwrite, degauss, and destroy.

Organizations must be aware that each of the methods has advantages and disadvantages and works best for specific hardware. Choosing one solution to fit the entire organization's hardware infrastructure may not suffice. For example, a Solid State Drive (SSD) cannot be degaussed because it is a cell media not a magnetic media like the Hard Disk Drive (HDD). SSDs must either be destroyed and/or overwritten, methods with their own limitations[iv]. Smashing or drilling holes through a hard drive with power tools may not be enough, because data can be retrieved from a hard drive platter that has been physically damaged. The US Department of Defense (DoD) requires that before a hard drive is physically destroyed, it should be overwritten or degaussed.[v]

In addition to the cost of media sanitizing, organizations may accumulate associated costs for the secure storage of drives until they can be processed, and assuring that the data wipe was successful or that the hard drive is so completely destroyed that absolutely no data can be rendered from it. Organizations with a heterogeneous mix of hardware can expect even higher associated costs due to the need for varied solutions and verification methods.

NIST agrees that as technology changes and new drives such as SSDs and SEDs make a big entry into the market place, new sanitization technologies may need to be applied[vi]. A new media sanitization method being considered in the industry is called crypto erase. In an article entitled *Data Security in Flash Devices* by the Trusted Computing Group (TCG) explains that "enhanced secure erase using key erasure is the preferred method"[vii]. Crypto erase offers organizations a secure, immediate, and auditable solution for re-purposing and disposing drives that house data of any security category. The crypto erase function is available at no additional cost with most encryption solutions.

Challenge

How can administrators ensure that all drives are sanitized sufficiently and how can IT departments save money in doing so? The challenge is finding a solution that effectively handles the different technologies (HHD and SSD), does not cost a fortune, and leaves a sufficient audit trail.

Solution

Whether a hard drive will be repurposed or retired, all personal identifiable data must be completely removed from it. This section compares the three traditional methods to crypto erase in the categories outlined below.

Security goal

The security goal of each solution is to ensure that data on the supported media is not accessible by unauthorized users after it is either sanitized or destroyed.

The overwrite method uses software to replace previously stored data on a drive or a disk with a predetermined pattern of meaningless information. NIST suggests that most media can be effectively cleared of **non-sensitive** data with one overwrite[viii], but according to the US Department of Defense (DoD) 5220.22-M, disks must be overwritten a minimum of three times[ix].

Comparatively, degaussing is a method where magnetic media is placed in a machine called a degausser, which exposes it to a strong magnetic field that disrupts the recorded information. NIST agrees that degaussing is an effective method of sanitizing damaged or exceptionally large magnetic disks. Disks are usually rendered unusable after degaussing.

Physically destroying a drive to the point where the damage is so great that the hard drive cannot be re-connected without significant rework is a NIST approved method of destroying disks which house highly sensitive data. Organizations resort to this method when disks are broken or the technology is too old.

Although crypto erase is currently not an approved method of media sanitization, NIST is no longer opposed to the method[x]. Crypto erase is a function that overwrites the encryption key the DoD 5220.22-M approved number of times to ensure that the MEK/DEK is indecipherable. Without the MEK/DEK, data on the hard drive is instantaneously inaccessible.

Benefits

See the chart below to review the benefits of each method.

	Overwriting	Degaussing	Physical destruction	Crypto erase
Disk can be re-purposed	✔	Rarely		✔
Audit logs available	✔			✔
Quick (under 10 minutes per drive)		✔	When using a machine	✔
Support for Hard Disk Drives (HDDs)	✔	✔	✔	✔
Support for Solid state drives (SSDs)	Limited		✔	✔
Support for USB keys			Depends on the method	✔
Secures data in hidden partitions	Limited	✔	✔	✔
Recoverable by authorized personal				✔
Stand-alone solution	Not for top-secret data	Not when storage is required	Not when storage is required	✔
Remote administration				✔
Sanitizes damaged media		✔	✔	Data already encrypted *plus* delete MEK/DEK from database
Software only	✔			✔

Cost

Crypto erase is the most cost effective sanitization method because it is provided as part of most FDE solutions. There are no additional training costs associated with this method as Administrators were trained to administer the encryption solution when it was first acquired.

The cost of the traditional three methods can vary greatly depending on the type of solution organizations deploy. For example, the purchase price of a degausser can range from $2,700 to $52,700[xi] [2], plus the cost of staff training, machine maintenance, and auditing. Outsourcing this service may cost as little as $6 per drive[xii].

Hardware erasers can range in price from $500 to $18,000[xiii], while data sanitization software can be as cheap as $50 for individual licenses and about $500 to $2,000 for the professional versions[xiv]. Additional costs include staff training, human labor hours, and auditing.

A shredder can cost approximately $19,000[xv], plus staff training, auditing, and hauling and dumping costs, which can be significant, while outsourced shredding can range from $5 to $10 per hard drive[xvi].

Although outsourcing the traditional methods appears to be cheap, organizations must consider the additional costs of storage and ensuring that drives are secure while in transit and in storage. If data that was destroyed by a contractor somehow resurfaces, the organization is liable for the damages suffered by the injured parties.[xvii] Organizations must also be mindful of the fact that many government and corporate security policies require that unencrypted drives be overwritten or degaussed in house prior to allowing them to leave the premise.

[2] All prices are shown in USD.

Labor cost

Overwriting is a very time intensive procedure. For example, it can take approximately one hour to overwrite 100 GB; therefore, it can take about 5 hours to overwrite one 500 GB drive once. The DoD standard is 3 times, resulting in 15 hours of human labor to overwrite one 500 GB drive.

The second most time-intensive and physically exhausting method is physical destruction, when it is done without the aid of a machine or an outsourcing service. It all depends on the strength, method, and tools. Physical destruction should only be conducted by trained and authorized personnel wearing protective gear and must be verified by a knowledgeable witness.

The least labour intensive methods are degaussing and crypto erase. Most degaussing devices have a one minute cycle but it takes a knowledgeable person to operate the machine and witness the process to verify that the hard drive was sanitized correctly. Comparatively, it takes one FDE administrator less than 1 minute to crypto erase a drive.

Outsourcing any of the traditional methods will help to decrease the labor cost as long as a vendor has been identified, security procedures have been put in place, and a regular pickup schedule is set.

Human error

Below are the types of human errors that can occur when sanitizing a disk, and how each method's effectiveness can be verified in the event of an error.

	Overwriting	Degaussing	Physical destruction	Crypto erase
Sloppy processing	Costly to verify completion	Costly to verify completion	Costly to verify completion	Audit logs track completion
Unsupported media processed	Not as effective for SSDs	Not effective for SSDs	Methods vary for different media	Supports HHD, SSD, USB
Amount of care required	Process must be followed	Process must be followed	Extremely thorough methods	Process must be followed
Reversible	Possible if process is not complete, but costly	Irreversible	Irreversible	Reversible if MEK/DEK is still in database

Further information about the crypto erase method

Key benefits of the crypto erase method

- **Instant** - The crypto erase command deletes encryption key in milliseconds, so data is instantaneously inaccessible.
- **Free –** Included with some FDE solution.
- **Easy –** Encryption key can be deleted with one click from the database.
- **Support for hardware and software based encryption**
- **Heterogeneous environment support –** Enterprises with PC, Macs, and Linux clients can benefit from one solution.
- **Support for HHD and SSD –** Encryption security does not depend on the hard drive type.
- **Reversible** - Keep the software-based encryption key for the retention period in the event that you need data.
- **Stand-alone solution** - Does not need to be combined with another sanitization method.
- **Minimal risk of human error –** As soon as the command is initiated, the process is automatic; no additional human interaction is required to secure data.
- **Remote erase** - Can be done remotely when the user is connected to the network.

For laptops / desktops with FDE enabled, an administrator can sanitize a drive by sending the crypto erase command, which will systematically overwrite the MEK/DEK.

Crypto erase can be administered from a central management server, the client's machine, or at pre-boot authentication. The available methods of sending the command are dependent upon the encryption vendor's solution. After the command is executed, data will be completely inaccessible.

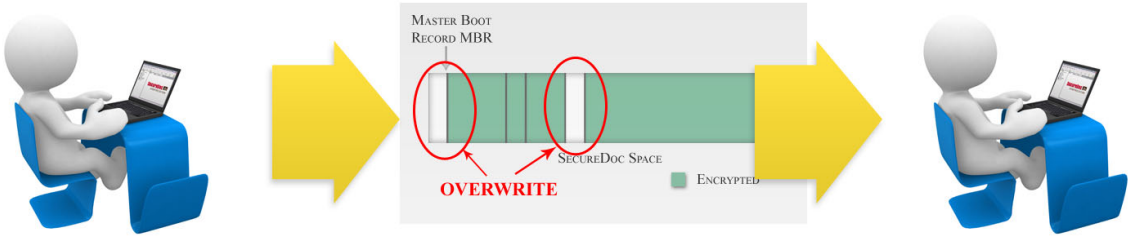
The most common way to commence the crypto erase command is from a central management server. Only administrators with permission to administer the command can sanitize the drive. Extensive audit logging documents the entire process. Administrators would crypto erase a computer from the central management server when an employee leaves the company, a laptop is stolen, or if the disk is retired, shipped to another office, or archived. A good encryption vendor will allow administrators to label their keys so recovery is easy, when needed. Some government or corporate policy may dictate that encryption keys must be deleted from the database and the database back up files must be deleted after the retention period passes to ensure no person has access to the retired data.

Authorized administrators can also initiate the crypto erase command directly from the FDE's administrative console on the client's machine or directly from the pre-boot authentication screen. The later method may be useful to protect top-security data on missions during an enemy attack. When data needs to be deleted immediacy, the user can press a predefined key stroke sequence which automatically crypto erase the drive. The enemy and the user will have no access to any of the encrypted data.

Access to crypto erased data can only be restored by an authorized FDE administrator with access to a copy of the original encryption key stored in a database or database backup file.

WinMagic offers all of the benefits of crypto erase functionality with its SecureDoc product. Below is an illustration of how SecureDoc's software and hardware FDE crypto erase function works.

Software-based encryption crypto erase



FDE Administrator sends crypto erase command from SES for selected online device.

Overwrites MBR and SecureDoc space so it is no longer identifiable on the drive.

Depending on the organization's security and retention policies, the encryption key can be manually deleted from the database.

Hardware-based encryption (OPAL SED) crypto erase

FDE Administrator sends crypto erase command from SES for selected online device.

Drive generates a new MEK/DEK and overwrites the old key.

Because the drive now has a new key and nobody has a copy, the drive is inaccessible.

WinMagic advantage

SecureDoc offers organizations one integrated, comprehensive software and hardware-based encryption solution to protect sensitive data across multiple platforms. Pedigree, innovation and customer satisfaction are part of our corporate fabric. We have set the bar with many industry firsts and have always been the first to successfully support many new technologies, including Windows 7, Vista, new computers, tablets, and new smartcard readers and smartcards.

Some of SecureDoc's key features include:

- Sector-by-sector full-disk encryption, except the MBR and SecureDoc space.
- Enterprise server management console that also facilitates key management.
- Single- and multi-factor pre-boot authentication using passwords, USB tokens, TPM, smartcards, biometrics, or PKI.
- Enterprise Server support for synchronization with Active Directory.
- Supports PC, Mac, and Linux clients.
- Supports the use of HDDs, SSDs, Self Encrypting Opal Drives, and Seagate Secure Drive.
- Writes detailed audit logs.
- Does not have a back door.

WinMagic has meets exceptionally high industry standards and has achieved internationally recognized security certificates.

- NIST Certificate #1 for AES
- FIPS 140-2 Level 2
- Common Criteria EAL-4
- BITS Certified
- First product to be approved by NSA to secure SECRET level data (SecureDoc for FORTEZZA)

Strong industry affiliations including:

- **Lenovo**
  The Lenovo-WinMagic strategic partnership ensures a flawless integration of SecureDoc's FDE with single- and multi-factor pre-boot authentication on Lenovo's notebooks and PCs.
- **Intel**
  WinMagic and Intel create strong comprehensive enterprise notebook security solutions that provide organizations with integrated data security and laptop theft prevention.
- **Apple**
  WinMagic and Apple have a strategic relationship to ensure interoperation.

- **Microsoft**
  WinMagic is a Microsoft Certified Partner and WinMagic® Inc. is part of Microsoft's Secure IT Alliance, which is a group of industry partners working together to develop security solutions for the Microsoft® platform.
- **Seagate**
  WinMagic has been designated as a Key Management Vendor for Seagate Secure.
- **Dell**
  WinMagic is the first encryption vendor to be named as a Dell Certified ISV Partner.

Fast Facts

- Sanitizing disks by deleting the encryption key is free.
- Data is inaccessible without the key.
- Secures PC, Mac, and Linux clients.
- WinMagic's SecureDoc allows administrators to manage encryption keys for the entire organization from one console.
- WinMagic's SecureDoc provides audit logging.
- Supports HDDs, SDDs, and Self Encrypting Opal Drives.

References

Andrew Kelleher, *Responsible Hard-Drive Destruction - Let's Get Real*, http://www.infosectoday.com/Articles/Hard_Drive_Destruction/Hard_Drive_Destruction.htm

Apple Insider, *Apple laying groundwork for TRIM support in future SSD-based Macs*, Jun. 2010, http://www.appleinsider.com/articles/10/06/14/apple_laying_groundwork_for_trim_support_in_future_ssd_based_macs.html

Data Destruction Products and Services, *Hard Drive Shredding Pricing*, http://www.semshred.com/content1315

Data Devices International, *Model 0300 Jackhammer Low/Medium Volume Hard Drive Shredder*, http://www.datadev.com/hard-drive-hdd-physical-destroyer.html

Department of Defense Inspector General, *Sanitization and Disposal of Excess Information Technology Equipment*, Report No. D-2009-104, Sep. 2009, http://www.dodig.mil/Audit/reports/fy09/09-104.pdf

dotHILL, *Solid State Drive Technology*, 2010, http://www.dothill.com/assets/pdfs/SSD_Solution_Brief.pdf

Experture and Robert Frances Group, *Balancing Hardware End-of-Life Costs and Responsibilities*, Dec 2007, ftp://public.dhe.ibm.com/common/ssi/ecm/en/gfl03037usen/GFL03037USEN.PDF

IBM, *Hard Drive Disposal: The Overlooked Confidentiality Exposure*, Nov. 2003, http://www-03.ibm.com/financing/pdf/us/recovery/igf4-a032.pdf

Media Duplication Systems, *Hard Drive Degaussers*, http://www.mediaduplicationsystems.com/Degausser_Hard_Drive_Degaussers_s/103.htm

Media Duplication Systems, *Hard Drive Erasers*, http://www.mediaduplicationsystems.com/Hard_Drive_Erasers_s/319.htm

National Institute of Standards and Technology (NIST), *NIST Special Publication 800-88: Guidelines for Media Sanitization*, Sep. 2006, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Peripheral Manufacturing Inc., *Degaussing (Erasing) Service*, http://www.periphman.com/tape-and-media-services/degaussing.shtml

Privacy Rights Clearinghouse, *Fact Sheet 12: Checklist of Responsible Information-Handling Practices*, revised Oct. 2010, http://www.privacyrights.org/fs/fs12-infohandling.htm

SANS Institute, *The Ten Most Important Security Trends of the Coming Year*, 2006, http://www.sans.org/security-resources/10_security_trends.pdf

Seagate, *Drive Disposal Best Practices*, 2007, http://www.seagate.com/docs/pdf/whitepaper/Disposal_TP582-1-0710US.pdf

Simson L. Garfinkel, *Remembrance of Data Passed: Used Disk Drives and Computer Forensics*, Nov. 2004, http://www.usenix.org/events/lisa04/tech/talks/garfinkel.pdf

Simson L. Garfinkel and Abhi Shelat, Re*membrance of Data Passed: A Study of Disk Sanitization Practices*, The IEEE Computer Society, Jan/Feb 2003, http://cdn.computerscience1.net/2006/fall/lectures/8/articles8.pdf

Teresa Worth, *Overwriting Data and Wiping Drives is NOT the Best Way to Protect your Data!*, Seagate, Mar. 2010, http://enterprise.media.seagate.com/2010/03/inside-it-storage/overwriting-data-and-wiping-drives-is-not-the-best-way-to-protect-your-data/

Trusted Computing Group (TCG), *Data Security in Flash Devices*, Jul. 2010, http://www.trustedcomputinggroup.org/media_room/news/150

Thomas Coughlin, *Data Security in Flash Devices*, Gerson Lehrman Group, Jul. 2010, http://www.glgroup.com/News/Data-Security-in-Flash-Devices-49611.html

U.S. Department of Health & Human Services (HHS), *HITECH Breach Notification Interim Final Rule*, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

Wikipedia, *TRIM*, http://en.wikipedia.org/wiki/TRIM

Endnotes

[i] Privacy Rights Clearing House, *Chronology of Data Breaches Security Breaches 2005-Present*, http://www.privacyrights.org/data-breach, search criteria 2010/2009 PHYS, PORT, STAT.

[ii] U.S. Department of Health & Human Services (HHS), *HITECH Breach Notification Interim Final Rule*, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

[iii] Simson L. Garfinkel and Abhi Shelat, Re*membrance of Data Passed: A Study of Disk Sanitization Practices*, The IEEE Computer Society, Jan/Feb 2003, http://cdn.computerscience1.net/2006/fall/lectures/8/articles8.pdf

[iv]dotHILL, *Solid State Drive Technology*, 2010, http://www.dothill.com/assets/pdfs/SSD_Solution_Brief.pdf, page 3

[v]Department of Defense Inspector General, *Sanitization and Disposal of Excess Information Technology Equipment*, Report No. D-2009-104, Sep. 2009, http://www.dodig.mil/Audit/reports/fy09/09-104.pdf, page 1

[vi] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-88: Guidelines for Media Sanitization*, Sep. 2006, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf, page 6

[vii] Trusted Computing Group (TCG), *Data Security in Flash Devices*, Jul. 2010, http://www.trustedcomputinggroup.org/media_room/news/150

[viii] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-88: Guidelines for Media Sanitization*, Sep. 2006, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

[ix]Experture and Robert Frances Group, *Balancing Hardware End-of-Life Costs and Responsibilities*, Dec 2007, ftp://public.dhe.ibm.com/common/ssi/ecm/en/gfl03037usen/GFL03037USEN.PDF, page 4

[x] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-88: Guidelines for Media Sanitization*, Sep. 2006, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

[xi] Media Duplication Systems, *Hard Drive Degaussers*, prices quoted on website for Jan 10, 2011, 2011, http://www.mediaduplicationsystems.com/Degausser_Hard_Drive_Degaussers_s/103.htm

[xii] Peripheral Manufacturing Inc., *Degaussing (Erasing) Service*, prices quoted on website for Jan 10, 2011, 2011, http://www.periphman.com/tape-and-media-services/degaussing.shtml

[xiii] Media Duplication Systems, *Hard Drive Erasers*, prices quoted on website for Jan 10, 2011, http://www.mediaduplicationsystems.com/Hard_Drive_Erasers_s/319.htm

[xiv]Seagate, *Drive Disposal Best Practices*, 2007, http://www.seagate.com/docs/pdf/whitepaper/Disposal_TP582-1-0710US.pdf, page 3

[xv]Data Devices International, *Model 0300 Jackhammer Low/Medium Volume Hard Drive Shredder*, prices quoted on website for Jan 10, 2011, http://www.datadev.com/hard-drive-hdd-physical-destroyer.html

[xvi] Data Destruction Products and Services, *Hard Drive Shredding Pricing*, prices quoted on website for Jan 10, 2011, http://www.semshred.com/content1315

[xvii] Andrew Kelleher, *Responsible Hard-Drive Destruction - Let's Get Real*, http://www.infosectoday.com/Articles/Hard_Drive_Destruction/Hard_Drive_Destruction.htm

200 Matheson Blvd. West, Suite 201, Mississauga, ON, Canada L5R 3L7
Tel: (905) 502-7000 | Fax: (905) 502-7001
Web: www.winmagic.com | Email: inquiries@winmagic.com

This White Paper is provided for information purposes, and to promote active consideration and discussion of data encryption for removable media. It is not an exhaustive discussion of the issues, and should be considered only as a starting point for a more complete assessment methodology.

WinMagic provides the world's most secure, manageable and easy-to–use data encryption solutions. Compatible with all editions of Microsoft Windows Vista, XP, and 2000 as well as Mac and Linux platforms, WinMagic's SecureDoc protects sensitive data stored on portable media such as laptops and removable media including USB thumb drives and CD/DVDs. Thousands of the most security conscious enterprises and government organizations around the world depend on SecureDoc to minimize business risks, meet privacy and regulatory compliance requirements, and protect valuable information assets against unauthorized access. With a full complement of professional and customer services, WinMagic supports over three million SecureDoc users in approximately 43 countries. For more information, please visit www.winmagic.com, call 1-888-879-5879 or e-mail us at info@winmagic.com.