

# **9 Keys to Comprehensive Enterprise Security**

A Simple Guide for IT & Security  
Administrators

.....

*September 2009*

### Securing data-at-rest in today's enterprise.

Sensitive data, from trade secrets to customer data, is more valuable and hence, more vulnerable than ever. Securing the data stored within the enterprise can be challenging in dealing with the heterogeneous nature as to where this information can be stored. In addition, dealing with the deployment of an enterprise encryption solution in conjunction with balancing administrator needs and end-user needs can be complex.

However finding the simplicity in this complexity is the balance sought by many enterprises in making it easy to deploy and manage data-at-rest encryption solutions. Confronted with enterprise owned PC Windows and Mac clients, and integrating new technologies to the enterprise (in the form of self-encrypting drives) can be difficult for IT security professionals especially when evaluating a new encryption solution that is easy to deploy and manage while addresses all the risks at the same time.

There is a staggering range of places where this data can reside and defending that data with the appropriate tools is a mounting challenge to IT and security professionals. Just the 'authorized' locations where this data might reside (laptops, desktops, CD/DVDs, removable hard drives, etc.) can be a challenge on its own. When you factor in all of the other devices with storage capacity that are owned by the employees, and not the enterprise (SD Cards, USB thumb drives, etc.), the risks and challenges rapidly multiply.

Regulatory and governance requirements are an increasingly important driver in the need to protect sensitive data. Companies are being required to disclose breaches that place Personal Identifiable Information (PII) at risk, be it from a customer, employee, shareholder, partner, or other stakeholder prospective. The amount of legislation is significant and accelerating. California's SB1386 (which requires public disclosure when unencrypted private data is potentially exposed) was an early benchmark, and in the United States today, 45 states have their own privacy and data breach legislation. This trend is not limited to the US – the EU Data Protection Directive and Japan's PIP Act also protect personal information. For the multinational organization, this growing range of legislation presents a significant risk and compliance challenges that will only increase.

As more and more enterprises turn to full-disk encryption (FDE), it has quickly become the De facto standard as an established technology to protect sensitive data and help achieve compliance with regulatory requirements. FDE solutions can render the data on lost laptops and removable media completely inaccessible to unauthorized personnel – radically reducing the risk associated with data breaches.

The trick with encryption is not just using it – encryption is a well-understood field and there are many options available to encrypt hard drives, removable media, and other places where sensitive data may

reside. The trick is deploying encryption reliably and effectively across the entire enterprise in a way that:

- Reduces calls to the help desk;
- Scales with existing IT architecture including Active Directory;
- Can be deployed relatively quickly and flawlessly;
- Helps satisfy regulatory/governance requirements;
- Will not disrupt the productivity of users; and
- Manages end-points with a low total cost of ownership.

This paper will review nine key criteria for evaluating an encryption platform that achieves comprehensive enterprise security for data-at-rest.

**Key #1: Know what you want**  
*(Doing your homework upfront will save you time and money.)*

Often, organizations looking at evaluating encryption products do not have clearly defined criteria on how to evaluate solutions in the market place. Having specific criteria in place can assist you and your organization in making the right choice for your IT environment.

For US Federal government agencies and departments including local and state governments, the criteria are clearly laid out in NIST SP 800-111. The US Federal evaluation criteria discussed in this special report can be summarized into the below sections:

- Storage encryption must use existing system features including OS and infrastructure: TPM, multiple platforms, multiple encryption schemas
- Centrally managed for all deployments of storage encryption: Central configuration, deploy and manage multiple encryption and removable media
- Cryptographic keys are secured and managed properly: FIPS, CC, Open standards of key storage, encrypted, authenticated
- Utilize appropriate user authentication methodologies: HSPD-12
- Implement measures to support and complement storage encryption for end user devices: Educate end users, set forth IT data security governance that can be enforced

In the commercial market segment, the evaluation criteria used by a majority of security conscious organizations seem to gravitate around the set of requirements below:

- I. Comprehensive Data Security:  
Data-at-rest encryption solutions must be able to support the heterogeneous nature of IT networks from “normal” drives to self-encrypting drives, from the various PC Windows platforms to the Mac operating system, and from encrypting the hard drive to encrypting removable media.
- II. Enterprise-Class Key Management:  
Ability to escrow encryption keys, dynamically provision them to authorized users and label the encryption keys for easy identification.
- III. Business Process Integration:  
Ability to define and enforce IT governance surrounding password

- rules, policies for encryption and management of removable media.
- IV. User Transparency:
  - Minimize end-user training, eliminate end-user involvement in deployment; reduce or eliminate call to the help desk
- V. Interoperability with IT Infrastructure:
  - Synchronization with Active Directory
- VI. Vendor Pedigree:
  - Security is a matter of trust therefore knowing who your vendor of choice is, what their associations are, and what their area of expertise is in dealing with data-at-rest are all extremely important

**Key #2: Strong and certified**  
*(It's about proving that you're using good encryption)*

The first thing you need to consider is the kind of encryption you will be deploying in terms of strength of the algorithm and the certifications associated with the crypto engine.

**How strong is strong?**

The recommended encryption standard is a system that offers Advanced Encryption Standard 256-bit encryption. AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. As of 2009, AES is one of the most popular algorithms used in symmetric key cryptography. Data encrypted with AES-256 encryption is secure enough that it is the first publicly accessible and open cipher approved by the NSA for top secret information.

**FIPS: Proving you're strong**

The Cryptographic Module Validation Program (CMVP) is operated jointly by the United States Government's National Institute of Standards and Technology (NIST) Computer Security Division and the Communications Security Establishment (CSE) of the Government of Canada. Validated crypto modules are required and/or recommended for most usages by governments and many enterprises define their policies based on the government standards.

FIPS validation is challenging to achieve both technically and fiscally. There is a standardized battery of tests as well as an element of source code review that must be passed over a period of several days. The cost to perform these tests through an approved laboratory can be significant (e.g., well over \$100,000 US) and does not include the time it takes to write, test, document and prepare a module for validation. After validation, modules must be resubmitted and re-evaluated if they are changed in any way.

A solution chosen to protect sensitive data-at-rest should use a cryptographic module that is FIPS 140-2 certified.

### **EAL: Proving you're well-designed and secure**

The Evaluation Assurance Level of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation. A higher number means greater requirements that must be met to achieve the certification. Most of these requirements involve design documentation, design analysis, functional testing, or penetration testing. The higher EALs involve more detailed documentation, analysis, and testing.

A solution chosen to protect your data should have Common Criteria EAL-4 certification.

### **Key #3: What you should encrypt** *(Hint: It's EVERYTHING)*

So you have strong, certified encryption. The question becomes: how do you use it to protect data on your laptop hard drives? (The type of encryption is the #1 concern for most organizations when they first deploy: FDE encryption versus file/folder encryption; software versus hardware based encryption.)

There are two main styles of encryption on the market today. The most prevalent form, and acknowledged best practice, is to encrypt the entire hard drive. This is known as FDE. The minority approach in the marketplace is file-based and may be known as 'file and folder encryption', 'full data encryption' or 'file system encryption'.

### **Full-Disk Encryption (FDE)**

FDE means what it says – the full disk is encrypted sector by sector, and there is no data stored on the disk that is unencrypted. Typically the encryption works "inline" once the user authenticates to the machine, and data is encrypted and decrypted as part of the read/write processes interacting with the hard drive. Efficient AES-256 crypto modules impose a low overhead to these processes and for typical users, the performance hit is not apparent. The authentication typically occurs in the pre-boot phase (i.e. before the operating system is launched) and if authentication fails, no data is exposed.

More recently, hard drive manufacturers have begun to offer hardware-enabled FDE – rather than requiring software based encryption to "convert" the drive to an encrypted drive, the disk ships from the factory in an encrypted state and all encryption/decryption happens inline in the drive with even better performance than is possible with software FDE (software is still required for pre-boot authentication (PBA) to activate the drive, central management and recovery of encryption keys if you plan to deploy to more than a handful of systems). The Seagate Momentus drives and new 'Opal' specification drives from other manufacturers underscore the fundamental validity of this approach, and they simply offer the full-disk encryption in an embedded hardware format. The advantages of self-encrypting drives include:

- Encryption time of hard drive eliminated
- More secure – no cooled boot RAM
- Better TCO – encryption time
- Self-encrypting drives will be the only option available
- In-line encryption quicker
- Sub layer of hard drives offer more protection: SecureDoc space hidden

However, hardware based encryption does not stand alone. Although the drive is shipped pre-encrypted, the drive needs to be centrally managed in the enterprise and in all likelihood needs to be managed with “normal” drives already present within the enterprise. The reality is that these self-encrypting drives require activation through PBA, central management and in order to complete the encryption solution, it needs to incorporate the encryption of removable media as data will be transferred off of the hard drive to USB thumb drives. In addition, in some sectors that lack encryption certification on these drives, it makes them less desirable, as other issues of dealing with legacy drives, retrofit options and availability add complexity to their use. In general, the manufacturers of self-encrypting drives face the following challenges that can only be resolved by using software base encryption alone or in conjunction with hardware based encryption:

- Strong PBA
- Removable Media Encryption
- Dealing with legacy drives
- Adoption (multi-sourcing and standards)
- Certification
- Key Management and Escrow
- Enterprise barriers include:
  - General availability
  - Retrofitting all laptops and workstations not plausible
  - Refresh cycles/policy may delay such deployments
  - Pre-imaging of drive may pose limitations
  - Pricing of these drives are currently more expensive

### **File / Folder Encryption (FFE)**

File-based encryption vendors are the minority and tend to spend a lot of time seeding fear, uncertainty and doubt about FDE. The majority of the claims made about the risks or limitations of FDE tend to be either inaccurate or are based on stale data from FDE solutions a decade or more old. File-based encryption systems typically leave portions of the hard drive unencrypted and this represents risk – unencrypted space means potential vulnerability. While sensitive files or folders may be encrypted, copies or portions of sensitive data still reside in temp files, swap files, spooling files, paging files and other areas used by the operating system or applications can leave the sensitive data vulnerable (and put the organization at risk). In many cases, encryption is left to the user to decide – they must choose to save files to the ‘secure area’ and mistakes or deliberate misuse can leave data vulnerable as well.

This type of technology is clearly file centric rather than device centric leaving vulnerability gaps for data breach exposure. One of these gaps also includes the exposure of the file name. Since a great deal can be ascertained about the data contained in a file by the file label, data breach notification goals may not be obtained using this method. For example, losing an unencrypted USB thumb drive with an encrypted file (folder) still leaves the file name exposed. Anyone finding the USB thumb drive can immediately detect that a file is on it and that the file name is "XYZ\_Payroll\_2009.xls". If this were leaked to the press, what will be undoubtedly reported is that a USB thumb drive with the payroll records for 2009 was lost – without any mention of the fact that the file was encrypted. This would therefore defeat the goal of keeping the organization's name from the press. At the end of the day, quasi FDE is not full-disk encryption and rather quasi security.

Governments and industry analysts agree that FDE is the best practice and most secure means of securing data-at-rest on laptop hard-drives and other vulnerable end-points. If you're going to encrypt your machines, you should encrypt everything on them. This eliminates the exposure of unencrypted space containing sensitive data, and removes elements of human error in exposing sensitive information. In addition, organizations looking to comply with governing privacy and security legislation are asked to check the exemption clauses under those regulations affecting them as FFE may not be enough to meet exemption requirements given that some of the data may still be at risk of exposure.

#### **Key #4: Encryption Needs Authentication** *(Without authentication, encryption is pointless)*

If encryption is like a strong vault for your data, then authentication is the key that opens the door to the vault. You can have the most powerful encryption system in the world protecting your data, but if your end-user's password is "p a s s w o r d", then your data isn't very safe.

Access security does not stop with the strength of the password. Authentication is the means by which a user verifies to the encryption system that he or she is authorized to access the protected data. There are five basic ways that you can provide authentication:

1. Something you know (i.e. you know a password).
2. Something you have (i.e. you have a smartcard or token).
3. Something you are (i.e. your fingerprints match those on file).
4. Where you are (i.e. you are on an authorized local network).
5. Someone who trusts you (i.e. an already-authorized person validates you physically or virtually).

A good encryption system will, at minimum, support strong passwords (i.e. not using your username, or 'password' or common dictionary words, requirements for uppercase/lowercase/number/ special characters, etc.). Coupled with the functionality to lock out a system

after a restricted number of failed attempts, a strong password is a good first line of defense in protecting sensitive data.

Other means of authentication include smart cards, USB tokens, TPM and biometrics that provide flexible and convenient means to authenticate, or added security through multi-factor authentication. A strong password or possession of a valid hardware token can both be good security measures on their own. Requiring knowledge of a password AND possession of a token at the same time greatly increases the security of the secure data.

For organizations that already use smart cards or biometrics to secure access to their buildings or secure areas, combination of these authentication methods with passwords can be an effective means to ensure seamless 'door to desktop' security.

In selecting an encryption solution, IT and security administrators should critically evaluate what authentication methodologies are supported (and validate that the support works as advertised with live software... not just on the vendor website).

Other issues surrounding end-user authentication involve Single Sign On (SSO) capabilities. As mentioned earlier in this whitepaper, traditionally an inverse relationship has existed between endpoint security and end-user productivity. In order to not affect end-user productivity, some organizations look to SSO as one way. While some endpoint encryption solutions provide this capability, SSO may not always adhere to IT data security governance.

Furthermore, some organizations have looked at automatically enabling PBA thereby effectively by-passing this feature. While this function can be technically achieved, by-passing PBA renders the entire enterprise data-at-rest encryption solution impotent as data can no longer be protected against unauthorized users with the exemption of a pre-boot network authentication methodology.

#### **Key #5: Encryption in the enterprise** *(Encrypting one laptop is easy; encrypting a thousand laptops is not)*

If you need to encrypt one, two or a dozen laptops, there are open source options that may do a 'good enough job' for your needs. This isn't to say that it will be the most secure, convenient, productive, or cost effective option (yes, free does have a cost in a TCO analysis), or that you will be assured of compliance with governance and regulatory requirements (including audit logs). But if you just need to do the bare minimum, then options DO exist.

However, if you need to not only encrypt but also PROVE that you encrypted hundreds or thousands of laptops, you have another kind of problem. This compounded with other pending IT issues within the enterprise when encryption solutions are not expected to affect internal end-user productivity. Typically the more secure an encryption

solution, the less productive it is for the end-user to use. Selecting an encryption solution that can provide the greatest amount of security without affecting end-user productivity is the most desired.

Enterprise-class encryption solutions will offer centrally-managed configuration, deployment and management over all of the encrypted endpoints in your organization. If your organization uses Microsoft's Active Directory or the Lightweight Directory Access Protocol (LDAP) for managing users and groups, a good enterprise encryption solution will synchronize with your existing system to help define and manage groups of users' encryption privileges.

A centralized encryption management console should provide the ability to define user and group privileges, push installation packages out to users for deployment, and manage the encryption once it is live, including password recovery, updates to users or permissions, and publication of updated policies or configurations. In order to increase productivity and end-user adoption, these functions should incorporate self-help utilities to reduce calls to the help desk and making it easy for the end-user to get access in the event they forgot their password.

In addition, the capability of sharing encryption keys and/or dynamically provisioning them when desired is of great value to the enterprise looking to increase end-user productivity, lower their total cost of ownership, and gain greater end-user adoption. One user case for this would be the use of removable media within the enterprise. There are generally 3 user cases that enterprises wish to address: (1) the sharing of USB thumb drives with authorized users, (2) the sharing of these devices with unauthorized users or loss of these devices internally, and (3) the loss of these devices external to the organization.

In case 1; users belonging to the same OU structure within Active Directory can have encryption keys dynamically provisioned to them thereby gaining instant access to encrypted mobile devices as if they were unencrypted with NO PASSWORDS REQUIRED. In case 2; individuals who are not resident within the same OU structure within Active Directory will not be able to obtain the appropriate encryption keys and therefore be denied access to the encrypted mobile device. In case 3; the device is entirely encrypted sector by sector and therefore unauthorized users are simply denied access to the device. Because the USB thumb drive is encrypted sector by sector, not only is that data file encrypted but data file name remains undetectable (a lot can be ascertained about the data content of a file by the name it is given – encrypt everything sector by sector).

**Key #6: Encryption shouldn't hurt**  
*(If encryption prevents productivity, you're in trouble)*

Any technology designed to protect data from unauthorized access is going to have some potential impact (at least if it is to be effective). Accessibility and security are a zero-sum game. The real trick with data security and encryption is establishing protection without getting in the way of the users continuing to do their jobs. In addition, end-user training should be minimal (if it is needed at all).

Part of this is the inevitable 'lost password'. At some point, users are going to forget their passwords or misplace their authentication tokens. Physical hardware issues are also a factor – power surges or dropped machines may corrupt portions of encrypted hard drives. The question becomes, 'how fast and easy is it to recover from these challenges?'

Enterprise encryption solutions should provide for distributed help-desk functionality to permit authorized users alternate means to access their encrypted laptops, either by resetting passwords or by providing one-time-use alternate authentication in the event of lost/forgotten tokens or smartcards. Looking for data-at-rest solutions that have end-user self-help features (answering a pre-defined number of personal questions before access is given in the event of forgotten password) and a password hint feature is most desirable to help reduce calls to the help desk and allow authorized users a backup plan for immediate access to laptops if a password is forgotten.

On the physical-defect side, encryption solutions should interoperate with disk recovery and other utilities to permit the IT administrators to fix the drive or at least recover the data securely if the drive is not salvageable. When employing encryption solutions, having the capability to build bootable CDs that will provision a complete Win32 environment with network support, a GUI and a FAT/NTFS/CDFS file system support is critical when trying to recover from hard drive failures or errors.

In most enterprise scenarios, deployment is the biggest challenge and cause for failure when implementing data-at-rest enterprise encryption solution. In an ideal scenario, software is deployed silently where users won't even notice that encryption is installed... aside from authenticating in a slightly different way (i.e. at pre-boot), the users should be able to continue working on their laptops or desktops as before. The encryption solution should handle intentional and unintentional power interruptions in addition to preparing the Hard drive for conversion drive before hand. FDE solutions should also support recovery from Hard drive conversion process should a problem occurs.

When evaluating enterprise-wide encryption, you should evaluate the solution for its ability to recover from user and technology problems as well as the potential impacts on productivity.

A particular scenario that can cause problems is when multiple users share access to common encrypted drives or media. If users are to enjoy the productivity benefits of shared resources, the encryption must not get in the way. Therefore, FDE solutions must accommodate multiple users per device and ensure that the data created by one user is protected from other users of the device and only shared among authorized users.

**Key #7: It's about more than hard drives**  
*(If it connects to the hard drive, it's a risk)*

Encrypting the hard drives of laptops is a great first step in achieving data security – but it's not the only step. What about the USB thumb drive on a keychain that is used to swap files between laptops? What about the mp3 player or the digital camera that is attached to the laptop? What about the DVD burner in that laptop?

Consideration of the effects of removable media needs to be part of any comprehensive data security initiative.

There are multiple options available for encryption of removable media.

1. Software-based "Sector-by-Sector" Encryption ('FDE for media'), where standard media is encrypted using software.
2. Hardware-based "Self-Encrypting" USB Drives, where special media is encrypted right from the manufacturer.
3. File and Folder Encryption (FFE), where individual files and folders are encrypted on the media.
4. Container Encryption, where an encrypted portion or partition of the media is encrypted.
5. Self-Extractor Encryption, where the media is not encrypted but can be used to transport encrypted self-extracting archives.

There are pros and cons to each of these options. IT and security administrators must critically evaluate the user cases and user stories within their organization to determine what the most effective methods for protecting data on removable media.

Related to removable media encryption are the notions of port control and disk access control. Port control can permit the administrator to 'lock down' access to devices and prevent connection to non-approved media. The less-common disk access control can intercede at the level of read-write activity from the drive and control the ability to read or write from any connected drives or media.

When evaluating a data-at-rest encryption solution, it is critical that the enterprise has a medium or device centric strategy to prevent data breaches and minimize the human errors involved in potentially exposing PII or sensitive data. The ideal choice for most enterprise administrators is to select an encryption solution that provides sector by sector encryption of removable media including CD/DVDs and SD cards, but also one that provides the capability to "white list" and/or

“black list” USB flash drive brands, models, and/or serial numbers belonging to these devices.

The savvy IT or security administrator will critically examine the RME capabilities of their chosen encryption solution for all of these options.

**Key #8: Key Management is key**  
*(How do you find or identify your key when you need it?)*

If you're encrypting a small amount of data using a few laptops, it is feasible to manually manage and protect the few cryptographic keys associated with the encrypted devices. As the number of encrypted devices expands across the enterprise it rapidly becomes impossible to do this manually. This becomes more evident as mature encryption users demand flexibility on creating their own encrypting keys for various devices and then dynamically share them to pre-defined authorized individuals.

But wait – it gets worse – with solid encryption, the loss of a key is basically the same as losing the data (today's vendors do not typically provide 'back doors' into their encryption solutions). Therefore, it is absolutely critical that there is a reliable means of capturing, storing and recovering the encryption keys. The ability to escrow encryption keys and label encryption keys for quick identification is critical to ensuring that information can always be accessed by authorized individuals.

Keys must remain accessible for the useful life of the data. In many cases this means at least the 7 years required for record-keeping by certain legislation as in the case of discovery. In other cases, this could mean decades. What happens if the person that knows the password forgets it after 6 years, or leaves the company, or passes away?

Enterprise-class key management requires that all of the keys established to protect the endpoint devices and media are centrally captured and escrowed. It also requires that authorized encryption administrators can rapidly and reliably find those keys again when they are needed – whether to help a user with a forgotten password, or to address inquiries from an auditor.

Not only must the system be reliable, but the key management system itself must be secure, otherwise all of the encrypted devices may be put at risk.

Any organization that is serious about enterprise-wide encryption must understand the key management capabilities of their chosen vendor and should seek demonstration of archive and recovery processes that will match their internal use cases and compliance needs.

**Key #9: Security within heterogeneity**  
*(Or, the challenges of encrypted apples and oranges)*

Despite the best intentions and efforts of some IT administrators, it is difficult to maintain platform and technology homogeneity across an organization, especially as the organization grows. There is always a new technology, an exception to the rule, or a special case that must be addressed.

Likewise in the encryption industry, there is a constant evolution to support new technologies and new requirements. On the authentication side, this is reflected in support for new tokens, smartcards and biometric devices. On the platform side, it means encryption support for new operating systems and device types.

An enterprise-class encryption solution should support heterogeneity across the deployed technologies and platforms. Ideally, a single solution should be able to manage encryption for:

- Hardware and Software encryption;
- Windows and Mac operating systems;
- Hard Drives and Removable Media;
- Support for 3<sup>rd</sup> party self encrypting devices;
- FDE, FFE and other needed forms of encryption.

If the solution cannot manage all these needs, IT security staff will face many challenges in managing multiple platforms and consoles, leading to greater total cost of ownership and increased risk of errors or noncompliance.

### SecureDoc from WinMagic (True enterprise-class encryption solutions)

SecureDoc is deployed at leading enterprises and government agencies, some of which includes tens of thousands of users (often in very heterogeneous environments). These organizations were able to deploy SecureDoc rapidly and effectively to protect their sensitive data.

#### ***SecureDoc assists in applying best practices in meeting the 9 keys to comprehensive enterprise security.***

#### **Key #1: Know what you want**

WinMagic's SecureDoc is FIPS 140-2 level 2 and Common Criteria EAL-4 certified. SecureDoc also possesses Certificate #1 from NIST, and is the first FDE solution to be approved by the NSA to secure SECRET level data. SecureDoc is the most flexible and comprehensive disk encryption solution available on the market today providing strong PBA. It also enables easy configuration, deployment and management of self encrypting drives and software FDE of legacy Hard Drives, on Windows and Mac clients through one enterprise management console. Also supports self-encrypting and normal encryption of removable media.

#### **Key #2: Strong and certified**

SecureDoc uses AES-256 encryption and its crypto engine is certified as FIPS 140-2 Level 2 and Common Criteria EAL-4. WinMagic has an extensive pedigree in high-security applications and even developed a solution that that was certified by the US National Security Agency (NSA) for protecting SECRET data within US government agencies (FORTEZZA based SecureDoc).

#### **Key #3: What you should encrypt**

WinMagic has been a leader in FDE since its founding in 1997. While FFE is an available option with SecureDoc, true FDE with PBA is the best practice and is fully supported by SecureDoc.

#### **Key #4: Encryption needs Authentication**

SecureDoc offers an industry-leading number of integrations with additional authentication methods including password, smartcards, tokens, biometrics, PKI and TPM. In fact, SecureDoc provides single or multiple factor authentication and was one of the first solutions with biometric authentication at pre-boot.

#### **Key #5: Encryption in the Enterprise**

SecureDoc Enterprise Server (SES) offers a central management console for SecureDoc that enables administrators to address the major needs of encryption in the enterprise. Key features include:

- User and group management that supports granular control over policy as it is applied to users;
- An advanced key management system that provides creation, administration, escrow and recovery of encryption keys;

- Software distribution tools that accelerate and simplify deployment;
- User support tools that reduce administrative overhead and ensure users remain productive;
- Audit logs and reports that provide proof of compliance and support for discovery processes.

#### **Key #6: Encryption shouldn't hurt**

SecureDoc enhances user experience and removes encryption complexity in the IT environment. Users should be able to do the same tasks before and after encryption. SecureDoc not only offers superb support for help desk and user support but also offers unparalleled support for group keys and a unique 'key on demand' functionality, enabling users to share resources and removable media seamlessly – with NO PASSWORD REQUIRED!

#### **Key #7: It's about more than hard drives**

SecureDoc offers not only FDE but also removable media protection, all within the same software license. Rather than requiring multiple systems or additional costs to encrypt removable media after laptop encryption is established, SecureDoc users can simply encrypt their removable media – all for less than the cost of some 'hardware-based' encrypted USB thumb drives.

#### **Key #8: Key Management is key**

SecureDoc Enterprise Server functions as a robust and reliable key management system, providing a secure central repository for all encryption keys used to protect hard drives, removable media and other encrypted endpoints managed by SecureDoc. A unique system of human-readable key names in the SecureDoc catalogue of encryption keys greatly simplifies recovery of archived keys and reduces the cost of compliance with audits and governance requirements.

#### **Key #9: Security within heterogeneity**

No other vendor matches the scope of support for heterogeneous encryption requirements when compared to WinMagic. With one encryption solution, SecureDoc delivers:

- Support for Seagate Momentus drives and Opal-specification drives from other manufacturers in addition to the software FDE from SecureDoc.
- Encryption for Windows (2000/XP/Vista) and Mac (OS X) operating systems, manageable and deployable from the same central server and including support for hardware or software encryption on both platforms.
- FDE plus software-based sector-by-sector encryption of removable media as well as port control and disk access control for complete protection when it comes to removable media.
- Available options including FFE, container encryption, self-extracting archives to extend the protection beyond hard drives and achieve separation of duties or defence-in-depth within encrypted drives.



200 Matheson Blvd. West, Suite 201, Mississauga, ON, Canada L5R 3L7  
Tel: (905) 502-7000 | Fax: (905) 502-7001  
Web: [www.winmagic.com](http://www.winmagic.com) | Email: [inquiries@winmagic.com](mailto: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](http://www.winmagic.com), call 1-888-879-5879 or e-mail us at [info@winmagic.com](mailto:info@winmagic.com).

SecureDoc, SecureDoc Enterprise Server, Compartmental SecureDoc, SecureDoc PDA, SecureDoc Personal Edition, SecureDoc RME, SecureDoc Removable Media Encryption, MySecureDoc, MySecureDoc Personal Edition Plus, MySecureDoc Media, and SecureDoc Central Database are trademarks of WinMagic Inc. Other products mentioned here in may be trademarks and / or registered trademarks of their respective owner.

© Copyright 2009 WinMagic Inc. All rights reserved. This document is for informational purpose only. WinMagic Inc. makes NO WARRANTIES, expressed or implied, in this document. All specification stated herein are subject to change without notice.