# Data Encryption Demystified:
Seven Common Misconceptions and the Solutions That Dispel Them

WINMAGIC®
DATA SECURITY

## Table of Contents

IT professionals at the enterprise level frequently turn to encryption for protecting data — throughout its life cycle — from theft or loss. Although encryption is a proven technology that delivers strong, effective data security, common myths and misconceptions about it persist, even among some people who are generally knowledgeable about computers. All too often, the myths surrounding encryption are based on misunderstanding of the technology or on outdated concepts.

This paper examines common misconceptions about data encryption and describes how new approaches dispel earlier myths. WinMagic solutions demonstrate that a centrally managed approach to data security using current-generation processor capabilities and modern disk technologies can effectively meet enterprise requirements.

## Prevalent encryption myths and misconceptions

Common misconceptions about data encryption sometimes cause decision makers and IT groups to dismiss the technology. This, in turn, can place corporate assets at risk and can sometimes present legal liabilities. This paper addresses the following seven misconceptions:

1. The password used to log in to a computer through the operating system is sufficient protection.
2. Data encryption slows down computer and network performance and reduces user productivity.
3. Encryption creates major IT headaches because of the difficulty in planning, deploying and maintaining.
4. Comprehensive encryption solutions for enterprises are too expensive.
5. Encryption that is built into the operating system makes additional encryption unnecessary.
6. There is no compelling reason for encrypting personal or corporate data.
7. IT departments can't realistically manage the vast assortment of mobile computing devices in use, so why even bother trying?

Though some of these statements may have been true in the past, enterprises operate in a very different environment today. Regulatory challenges — regardless of the country or locality in which your company operates — cannot be overlooked without risking penalties and fines. More sophisticated hacking tools and organized theft increase the threat of data breaches and laptop loss. And, increasingly, thieves find compact, mobile computing devices to be inviting targets. Unfortunately, these popular devices are not always included in an organization's data security strategy.

Recent technology advances, as well as smarter data security solutions, help counter these challenges and threats. For example, Intel has built new instructions into recent processors to streamline encryption operations. This diminishes the performance hit of using full-disk encryption. These Advanced Encryption Standard – New Instructions (AES-NI) deliver strong encryption based on the Rijndael symmetric block cipher algorithm. AES has been adopted by the U.S. National Institute of Standards and Technology for government use because of its efficiency and thorough protection.

Another technology advance — self-encrypting drives — make encryption and decryption largely transparent to users and IT administrators. Innovative approaches to theft protection based in hardware, including Intel Anti-Theft Technology, make it easy to remotely disable stolen computers, eliminating their value to thieves.

Technology by itself, of course, doesn't guarantee that data security challenges are adequately met. Even with the latest technologies available, enterprises require a solution that:

- Scales to the demands of many thousands of users
- Performs quietly in the background without annoying users
- Supports the best practices being used by the organization for data security
- Protects the full range of devices being used in the company — from smartphones and tablet computers to high-end laptops
- Makes it easy for administrators to deploy, monitor and maintain the security features

The following sections look at the seven misconceptions about data encryption and counter the basis behind them.

## Myth #1: Passwords adequately protect laptops

Superficially, it might seem as though a simple username and password is enough to protect a laptop when it is first powered on; in practice, however, this approach is woefully inadequate if a laptop is lost or stolen. With minimal expertise, a thief can easily remove the hard drive from the laptop and access the data contents from another system — assuming that the data is not encrypted. Even if the data is encrypted, if there is not some form of pre-boot authentication — external to the operating system — hackers can bypass or detect the sign-on password. A variety of common hacking tools can make short work of the username and password combinations that normally protect a laptop during login.

In comparison, strong data security solutions that rely on encryption protect everything on the hard disk. Even if the disk is removed and connected to another system, nothing on it can be read without the key. Modern encryption solutions often store the key in a protected area in hardware. This is a more secure approach than a simple password. It can be coupled with authentication techniques, such as a biometric reader or external token, to further strengthen the security. Additional security is provided if secure key management is centralized so that the key does not remain on the system, but is only provided when required from the central location. This is how WinMagic PBConnex™ handles key management.

Relying on password protection alone, without encryption, may be sufficient for casual computer use, assuming that the machine does not contain sensitive or private information. For enterprise applications, however, passwords alone are weak and unacceptable, nor are they a suitable method for meeting regulatory requirements.

## Myth #2: Data encryption slows performance and reduces productivity

Encryption has already become an integral part of many everyday computer activities. When someone enters a credit card number or personal data on a website, many sites use cryptographic protocols for the exchange. These transactions occur so seamlessly that users don’t even notice them taking place.

Historically, when computer processors were less powerful, data encryption significantly slowed system performance. Whole-disk encryption, in particular, resulted in discernible lags and slowdowns. To many users, this seemed like an unacceptable trade-off to pay for the benefits of data security. It also established data encryption in many peoples’ minds as a technology that caused poor performance. This effect was multiplied at the enterprise level when network operations were substantially affected, and encryption created bottlenecks that could be measured and tracked across nodes.

Encryption operations that were once performed in software can now be carried out more efficiently within the processor hardware. Such is the case with AES-NI instructions in the architecture of recent Intel and AMD processors.

Besides presenting greater resistance to hackers mounting side-channel attacks to break AES encryption, these special-purpose instructions reduce the number of machine cycles to accomplish encryption tasks. This results in performance increases of up to 50 percent for applications enabled for this hardware feature.

As a result, most users on modern systems don’t even notice that encryption is taking place. Although mobile computing devices — such as tablets, laptops and smartphones — don’t have the same processing capacities as desktop machines, typically even their processors can efficiently handle encryption operations fairly transparently. This proves to be an important characteristic for mobile devices, since enterprises are increasingly called upon to incorporate them into their data security strategy.

## Myth #3: Deploying data encryption solutions causes IT headaches

While many IT professionals advocate the universal use of encryption on all computing devices within an organization, most agree that these solutions must be implemented in a way that can be managed and monitored consistently, without requiring users to install or set up the features and options to be used. Accomplishing this requires both a well-designed encryption solution and central administrative management tools that deploy and maintain the encryption software transparently, with minimal impact on users.

Particularly for organizations with thousands of employees, data encryption solutions without a single point-of-control can be a challenge to plan, deploy, implement, service and maintain. Well-designed solutions offer a management console where administrators can install, monitor, track and maintain the data encryption solution. This ensures consistency in maintaining the highest standard to meet corporate and regulatory policies. It also eases the IT burden, particularly in comparison with solutions that require several different components, each with its own interface and controls.

### Transparency

Because earlier generation solutions lacked transparency, both users and IT professionals often rejected them. Today, transparency is an essential aspect of data security solutions, aided by advances such as self-encrypting drives, embedded hardware-based operations, and background encryption and decryption operations running in parallel on multiprocessors.

### Impact on IT operations

Software engineering and design can make the difference between an effective, easy-to-use solution and one that taxes the IT staff and places a burden on everyday activities and maintenance. Individual solutions should be compared on a point-by-point basis to see how they measure up. How well does an encryption solution fit into the existing IT infrastructure? Does it support all the computing devices in use? Does it simplify the process of documenting the security in use for regulatory purposes? Can encryption be administered in a uniform way throughout the organization? All of these factors weigh into the overall impact on IT operations. Solutions designed from the ground up to meet enterprise requirements typically fare better in these regards than point solutions.

### Changes of processes required

Many old-fashioned encryption solutions – even those from well-known vendors – offer outdated technologies when it comes to deployment or user authentication. Complex password reset mechanisms put an increased burden on administrators and end-users. In addition, such outdated solutions require administrators to temporarily disable all security when provisioning new software at night. They also force IT to specify in advance who might use a device, complicating the roll-out processes significantly.

A modern encryption solution however enables the administrator to manage an encrypted endpoint in the same way as an unencrypted one as long as it is connected to the corporate network, thereby dramatically reducing the total cost of ownership.

## Myth #4: Enterprise encryption solutions are too expensive

You can currently buy a laptop for as little as $300, but if the information on that laptop is compromised, the financial repercussions can dwarf that expense.

In one of the most comprehensive studies of its kind, the Ponemon Institute released a study that surveyed 329 private and public sector organizations in the U.S. Organizations that participated in the study ranged in size from fewer than 1,000 to more than 75,000 employees. The Ponemon Institute determined that the least significant aspect of the loss was the actual cost of replacing the laptop. Several factors amplified the severity of the loss:

- Detection (monitoring and discovering that a loss had occurred)
- Forensics (tracing the details and characteristics of a loss)
- Data breach repercussions
- Lost intellectual property, lost productivity
- Legal, consulting and regulatory expenses associated with a breach

Results of the financial loss assessments included these statistics:

- The average cost of the laptop losses of organizations surveyed was $6.4 million for each company.
- The total of the laptop losses for the 329 organizations, combined, was $2.1 billion.
- Forty-six percent of the participants said the lost laptops contained sensitive or confidential data, but only 30 percent were encrypted.
- The average cost per lost laptop, considering all factors, was $25,454.
- Use of encryption can reduce the cost per lost laptop by $20,000.

There are abundant examples of breaches that have caused long-term harm to the reputations of the companies involved.

In the year 2011 alone, laptop losses led to the following breaches[1]:

- At the Kansas Lawrence Memorial Hospital, a laptop loss disclosed financial information of more than 8,000 patients.
- More than 6,000 documents from HBGary Federal in Russia were stolen and published. This breach included corporate emails, presentations and client reports.
- A data breach at the University of South Carolina exposed 31,000 names, health records, financial data and social security numbers.

In another instance, the Science Applications International Corporation (SAIC), which bears responsibility for protecting the personal data of military personnel, lost more than 4.6 million records in September 2011 when an employee left back-up tapes unprotected in his car. The serious consequences of this careless mistake will taint the security reputation of SAIC for many years.

More cost considerations compiled from other surveys:

- Of the 256 laptops lost[2] by the average organization each year (as noted by an Information Week study in 2010), a company typically only recovers 12.
- In the United States, according to the 2010 U.S. Cost of a Data Breach study[3], the average cost of a data breach increased to $7.2 million and cost companies an average of $214 per compromised record.

Companies evaluating the costs of data encryption solutions should factor in the true cost rather than simply the relatively trivial cost of the hardware itself.

[1] The Ponemon Institute, The Billion Euro Lost Laptop Problem (April 2011)

[2] http://www.informationweek.com/news/security/mobile/229402043

[3] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon

## Myth #5: OS-based encryption protection is sufficient for enterprises

Encryption capabilities available through operating systems do offer some degree of protection against data breaches. But these single-dimensional solutions lack the rigor, manageability, cross-platform support and more comprehensive encryption features that characterize serious enterprise solutions.

For example, Microsoft's BitLocker, available in the Ultimate and Enterprise versions of Windows 7, can now encrypt entire volumes and it works with a Trusted Platform Module (TPM) chip. This strengthens authentication when this feature is used, but does it provide the features most enterprises find necessary for comprehensive data security? Unfortunately, because BitLocker relies on the Windows platform for authentication, it is open to many known vulnerabilities that require patching. BitLocker security requires the entry of a PIN, which is bound to the hardware. This is shared amongst all users of the machine. If a second machine is used by the user it will normally have another PIN leading to. Because BitLocker is for Windows only, it will not support Linux or Mac OS machines that may be in use within an organization. And, since it can be run without pre-boot authentication, it lacks protections that may be necessary to meet regulations when confidential documents or personal data are at stake. Many enterprises, who initially adopted BitLocker, thinking it was for free, returned to professional encryption solutions, as the total cost of ownership of BitLocker was far too high and user satisfaction low.

For enterprise data security, solutions that require the active involvement of users can be weakened when the users fail to follow practices or neglect to apply encryption to files or folders. Without central management, administrators cannot oversee or modify user behavior. From a regulatory perspective, there is no reasonable way to track or ensure that confidential data has been protected. In the case of loss or theft, without some means of validating that encryption was applied to the data in question, companies could be liable for violating privacy laws.

In the U.S., forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have laws[4] that mandate that whenever a data breach involving personal data occurs, the party involved in the breach must disclose this to everyone whose data was comprised. Clearly, this is more than an embarrassment to a company involved. It's something that can destroy confidence in the integrity of a company, which may take years to restore.

For complying with regulatory mandates, data security solutions that let administrators centrally manage the key operations, determine the data content to encrypt, and ensure that corporate policies and practices are being followed offer a more effective approach. When a centralized management approach is applied  the level of data security rises, since the likelihood of sensitive files remaining unencrypted diminishes.

[4] http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

## Myth #6: There is no compelling reason to encrypt data

Protection of assets — the primary reason for encrypting data — encompasses two major concerns that are fundamental to organizations of any size:

- Meeting the local, state and federal regulations that apply to the protection of private individual data, including health records, financial information, personal histories, employment status and similar information. Different regulations exist in different regions. Organizations are required by law to determine the regulations that apply and to ensure that the appropriate level of protection is maintained.
- Preventing unauthorized individuals from gaining access to information that could impinge on intellectual property issues, offer unfair advantages in competitive relationships, reveal sensitive product roadmaps, engineering plans or unpublished financial results, or put an organization in an uncomfortable position if exposed in the media. All of these factors can jeopardize an organization's status and, potentially, financial position.

When implemented properly, encryption of sensitive data can satisfy the requirements of most laws and mandates. Through monitoring and tracking, administrators must be able to demonstrate that the data protections were applied consistently, potential data breaches were flagged, and the sensitive data was managed in a way that did not leave vulnerabilities or the possibility of exposure wherever and whenever it was used, moved, or stored.

Data encryption backed by a solution that ensures organization-wide compliance serves these goals very effectively.

## Myth #7: IT departments have no practical way to protect mobile devices

The rising popularity of mobile computing devices creates a new imperative for data protection. No longer locked behind the security of a corporate firewall, laptops, smartphones and tablets now travel with their owners, and are often loaded with sensitive corporate data that could cause substantial financial loss and possible legal liabilities if exposed.

Incorporating mobile devices, as well as equipment that runs diverse operating systems, can be an IT nightmare unless a solution accommodates all types of computing devices in a uniform, consistent, manageable way.

Because employees may use a variety of mobile devices running on different platforms — Linux, Windows, Mac OS, iOS and Android — these devices need to be integrated into the infrastructure and data security strategy. Ideally, a data security solution must be able to let administrators monitor, upgrade and manage the encryption use and deployment. A mechanism for protecting mobile devices should be an integral part of any serious data security solution. Encryption of small form-factor devices — which include tablets, smartphones and netbooks — must be implemented with the same attention given to laptops and desktop machines. If this practice is not followed, data security breaches could trigger regulatory action or fines.

Modern solutions allow you to monitor the data security status of all devices used by a user, irrespective of the form factor or operating system used, within a single administration console.

## Technology advances that enhance data encryption operations

Several technology advances have brought encryption into more widespread use in the industry. WinMagic has incorporated support for these technologies in recent solutions:

- **Network aware pre-boot security:** WinMagic has introduced this revolutionary technology to eliminate the headaches that legacy solutions – even those from large vendors – are causing in their daily use. As the only solution on the market, SecureDoc allows you to authenticate users against the network even before the OS starts, eliminating complex password reset changes for users in the corporate network and the need to pre-provision accounts on encrypted endpoints. It also allows you to roll-out system updates at night without having to compromise security as other solutions require.
- **Improved encryption algorithms**: Modern encryption algorithms use longer keys for better data protection. By leveraging the current-generation processor technologies and more efficient encryption models to handle the more complex calculations, performance demands can be met.
- **Self-encrypting drives**: The widespread adoption of the Trusted Computing Group standard and the rising popularity of Opal-compliant self-encrypting drives accelerate encryption and decryption operations. It also provides an extra measure of hardware security and automation to the processes.
- **Embedded hardware mechanisms**: Performing critical operations and storing keys in secure areas in hardware overcomes prior vulnerabilities associated with software-only approaches to encryption and key storage. Authentication techniques that rely on built-in hardware features, such as TPM chips, are inherently more secure than software-only approaches.
- **Robust multifactor authentication methods**: Many advanced technology methods are currently available to prevent unauthorized individuals from breaking into encrypted systems. Examples of these techniques include biometric input, TPM, Smartcard, PKI and token.
- **AES-NI instruction support**: Processor instructions that streamline AES encryption operations have been added to Intel and AMD processors, substantially reducing the time required to encrypt and decrypt data.
- **Security validation standards**: Validation standards for cryptographic techniques — such as the Federal Information Processing Standard (FIPS 140-2), a requirement for federal government documents in the U.S. — provide a mechanism for assessing the protection level of hardware and software components. Organizations are able to select security solutions that meet their requirements by determining the level of validation.

These technologies have helped eliminate the problems that were the original source of many data encryption misconceptions.

## Technology and privacy regulations

Most privacy laws and regulations do not specifically dictate what form of technology must be applied to protect an individual's private information or sensitive corporate data. However, when implemented appropriately, data encryption is recognized worldwide as a valid and effective means of privacy protection.

Among the most important laws and regulations are these:

- Data Breach Notification Laws (implemented individually by 38 states in the U.S.)
- Data Protection Laws – Germany/UK
- European Union Data Protection Directive (EUDPD)
- Personal Information Protection and Electronics Document Act (PIPEDA) – Canada
- Gramm-Leach-Bliley (GLB) Act – U.S.
- Sarbanes-Oxley Act (SOX) – U.S.
- Health Insurance Portability and Accountability Act (HIPAA) – U.S.
- Health Information Technology for Economic and Clinical Health Act (HITECH) – U.S.
- PCI Data Security Standard (PCI DSS) - Global

IT administrators and security professionals need to understand all the laws and regulations in the regions where they do business and to apply the necessary security measures to avoid penalties or fines.

## WinMagic SecureDoc counters the data encryption myths

WinMagic SecureDoc™ provides comprehensive data encryption protection to a wide range of computing and storage devices. To stay ahead of the technology curve, SecureDoc has been engineered to take advantage of the latest hardware and software technologies. This includes Opal-compliant self-encrypting drives, modern encryption algorithms, multi-threading to take advantage of multi-core processors, AES-NI encryption processor instructions, secure hardware areas available in current-generation processors, and other advances. WinMagic's engineering excellence and commitment to enterprise security is demonstrated by FIPS 140-2 Level 2 and CC EAL4 certification for SecureDoc.

Collaboration between WinMagic and Intel has resulted in support for the AES-NI instructions. This lets encryption operations be accelerated at the hardware level, resulting in much faster performance and more transparency. By thinking ahead, WinMagic gained recognition as a "Visionary in Mobile Data Protection" in Gartner's Magic Quadrant.

If the computer is not equipped with AES-NI or an Opal drive, SecureDoc automatically provides high performance software for such legacy hardware. Even better: Linux and Mac OS computers can be protected and managed within the same administration platform. With our next release Android and iOS machines will be supported, enabling you to manage data security for all desktops, laptops, tablets, smartphones and servers with an integrated, simple to use approach.

WinMagic data security solutions work on multiple levels and address the typical challenges faced by large-scale organizations. Beyond the robust full-disk encryption features of SecureDoc, SecureDoc File and Folder Encryption (FFE) ensures that files and folders on individual devices or on the network are automatically encrypted and secured, using an advanced key management for each user and Active Directory groups. PBConnex, a component of SecureDoc, enhances administrative tasks by providing auto-boot services with the security of pre-boot authentication supported across the network. Even the smallest (and potentially most vulnerable) devices — such as USB sticks and removable hard drives — receive protection with SecureDoc Removable Media Container Encryption, which helps eliminate the risks of data leakage. And, on a large scale, SecureDoc Enterprise Server v5.3 gives administrators a single, integrated management console that can handle the full range of an organization's data encryption requirements, including configuration, deployment, monitoring and maintenance.

In real-world terms, the value of a data security solution to an enterprise comes down to how it functions in everyday operations and how effectively it integrates into the increasingly complex operating environments faced by many IT groups. In a recent article in SC Magazine, the editors evaluated WinMagic PBConnex and the SecureDoc Encryption Server in their "First Look" column and came to this conclusion[5]:

> "Overall, this is an extraordinarily flexible, well thought-out and effective application of encryption. We like it a lot, and it is well worth your consideration."

For more information about the comprehensive, enterprise-caliber data security solutions from WinMagic and the ways in which they can simplify data encryption tasks for users and IT, visit www.winmagic.com.

[5] http://www.scmagazine.com/enterprise-whole-disk-encryption-done-right/article/223636/

## About WinMagic

WinMagic’s SecureDoc full-disk encryption solutions make it simple to protect all data on desktops, laptops, tablets and removable media, including USB thumb drives, CD/DVDs and SD Cards. Compatible with Microsoft Windows 7, Vista, XP and 2000; Mac OS X Snow Leopard, Leopard and Tiger as well as Linux platforms, SecureDoc makes it just as easy to centrally manage and use standard drives and self-encrypting drives including Seagate and Opal-compliant drives. WinMagic is trusted by thousands of enterprises and government organizations worldwide to minimize business risks, meet privacy/regulatory compliance requirements, and protect valuable information assets against unauthorized access. With a full complement of professional and customer services, WinMagic supports over 3 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.