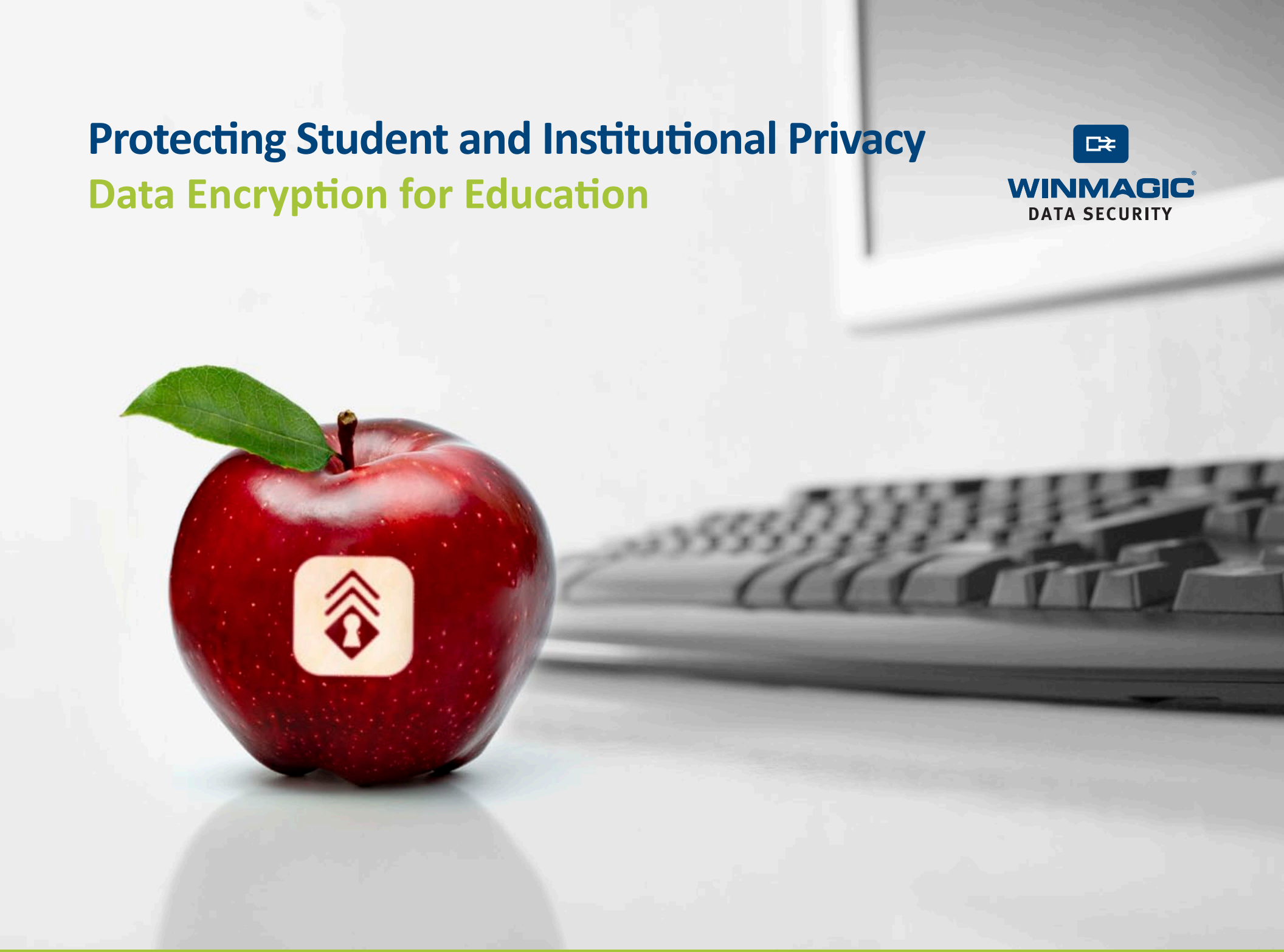
Protecting Student and Institutional Privacy

Data Encryption for Education

WINMAGIC®
DATA SECURITY



FOREWORD

WINMAGIC® DATA SECURITY

Schools, colleges and universities are facing data security issues on a regular basis and the nature of their IT systems present unique challenges. Balancing diverse information with required security control is complicated when the IT infrastructure is decentralized and difficult to manage. Adding to these challenges is a diverse user population and the increased use of multiple devices and platforms.

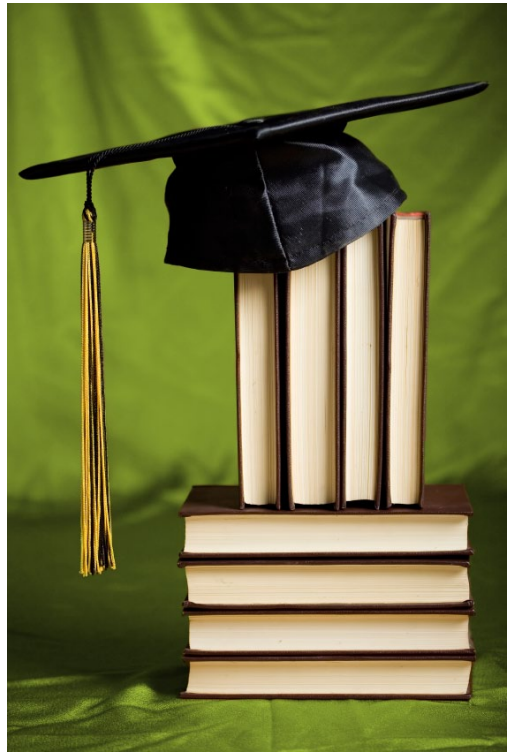
In this eBook, you'll discover the basics of data encryption; how it addresses the unique data security challenges facing educational institutions, and key points to consider when building the business case for data encryption. You'll also learn about some common "data encryption myths" and the risks they pose.

TABLE OF CONTENTS

INTRODUCTION

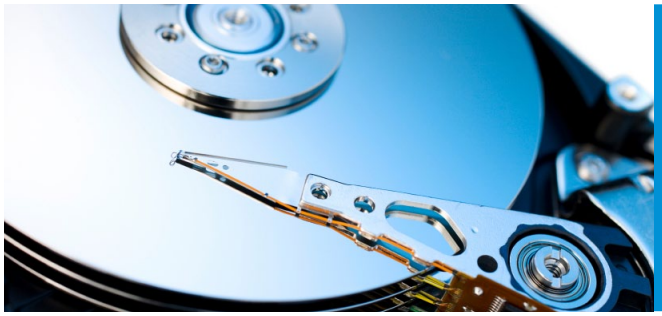
In a world with an increasing dependence on technology, the rapid user adoption of multiple devices as a way to conduct business productively has quickly become a reality for organizations. The notion of sitting behind a desk with a desktop computer has given way to laptops, tablets, smartphones, and other devices, whether they're owned by the individual or provided by the organization.

For educators, this reality is even more evident with faculty and students using a variety of platforms to research, learn, access and store information. Protecting this critical data presents a unique challenge given a school's diverse and ever-changing population, regulatory compliance issues around privacy of student records, along with providing secure access into course material and other data by remote and transitional users.



76% of employees use multiple devices, many of which belong to the individual, not the organization.

CHALLENGES FACING EDUCATIONAL INSTITUTIONS



The protection of sensitive information such as student and parent information, financial records, loans, employment records, and other important documents is paramount for educational institutions. For post secondary institutions, where information also includes research and large amounts of intellectual property, data security becomes even more critical.

The key challenges prompting educational institutions to consider data protection solutions are the need to:

- Protect sensitive data and personal identifiable information (PII) on multiple platforms and devices
- Employ flexible and centralized administration for a user base that changes from term-to-term
- Enable secure sharing of data with other institutions, research partners and other stakeholders

PROTECTING SENSITIVE DATA ACROSS MULTIPLE PLATFORMS

Today, a myriad of options exist for accessing and sharing information in schools. Laptops, tablets, shared workstations in classrooms and labs, USB keys and personal mobile devices all provide ways for students and staff to access and share learning materials and in many cases, sensitive information.

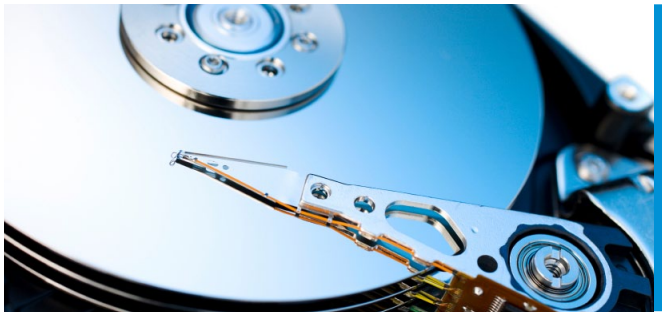
We've come to expect the seamless use of a variety of devices to access content, and just like corporate organizations, many schools are embracing the Bring Your Own Device (BYOD) trend and implementing policies that encourage their use. Why? The use of personal mobile devices can:

- Increase productivity in staff, faculty and students
- Provide flexible access to learning materials, like e-textbooks and apps, resulting in a more favorable learning environment
- Reduce IT costs because the devices are not purchased through the school

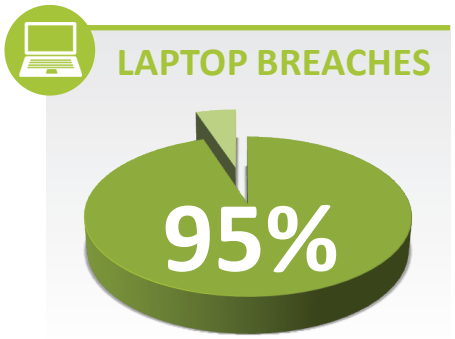
Even for those who aren't proactively implementing a BYOD program, the proliferation of devices is so widespread that campus' IT departments need to evolve to handle the growth. The challenge facing educators is how to develop an effective strategy to manage these disparate devices so that "Bring your own Device", doesn't turn into "Bring your own Disaster."

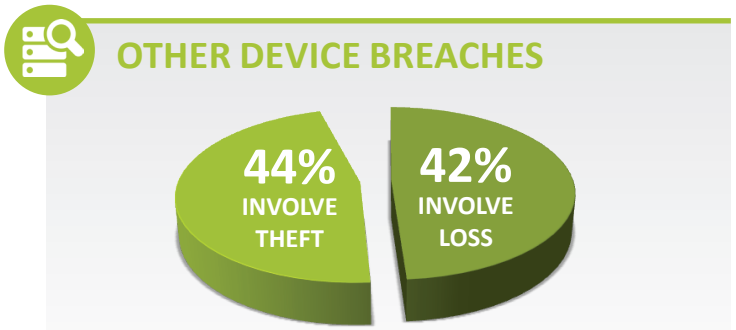
Educational institutions need a **cost effective**, **flexible strategy** to address their unique challenges.

CHALLENGES FACING EDUCATIONAL INSTITUTIONS



50% of breaches are from laptops or other compromised locations, such as mobile devices.





Source: Kaufman, Rossin & Co. 2012 Report

FLEXIBLE CENTRALIZED ADMINISTRATION FOR A CHANGING USER BASE

It's only natural that students come and go from term to term and that faculty members and administration move from school to school. When that happens, it's important to understand how this impacts data security. Without a system to manage all accounts and devices from a centralized location, it's virtually impossible to ensure the security of data on every device. With students and staff using an average of two to three devices simultaneously, the need for an operating system agnostic solution, with full mobile device management capabilities, from a central location is even more imperative.

SECURE SHARING OF DATA WITH OTHER INSTITUTIONS, RESEARCH PARTNERS AND OTHER STAKEHOLDERS

Despite a culture and mandate that promotes the sharing of data, educational institutions face the same issues as commercial enterprises when it comes to protecting personal identifiable information (PII). Educators need to be sure that their data is safe in the event that it falls into unauthorized hands.

These days, removable media devices are everywhere and capable of storing massive quantities of data, making it convenient to share information across a variety of devices in libraries, research labs or virtually anywhere a connection is available for access. The majority of schools have no control over the devices and the connection from which the data is being shared, leaving them at risk for leaks or having private data fall into the wrong hands.

So, where can educational institutions turn to for a cost effective, flexible strategy to address their unique challenges? The answer is **Data Encryption**.

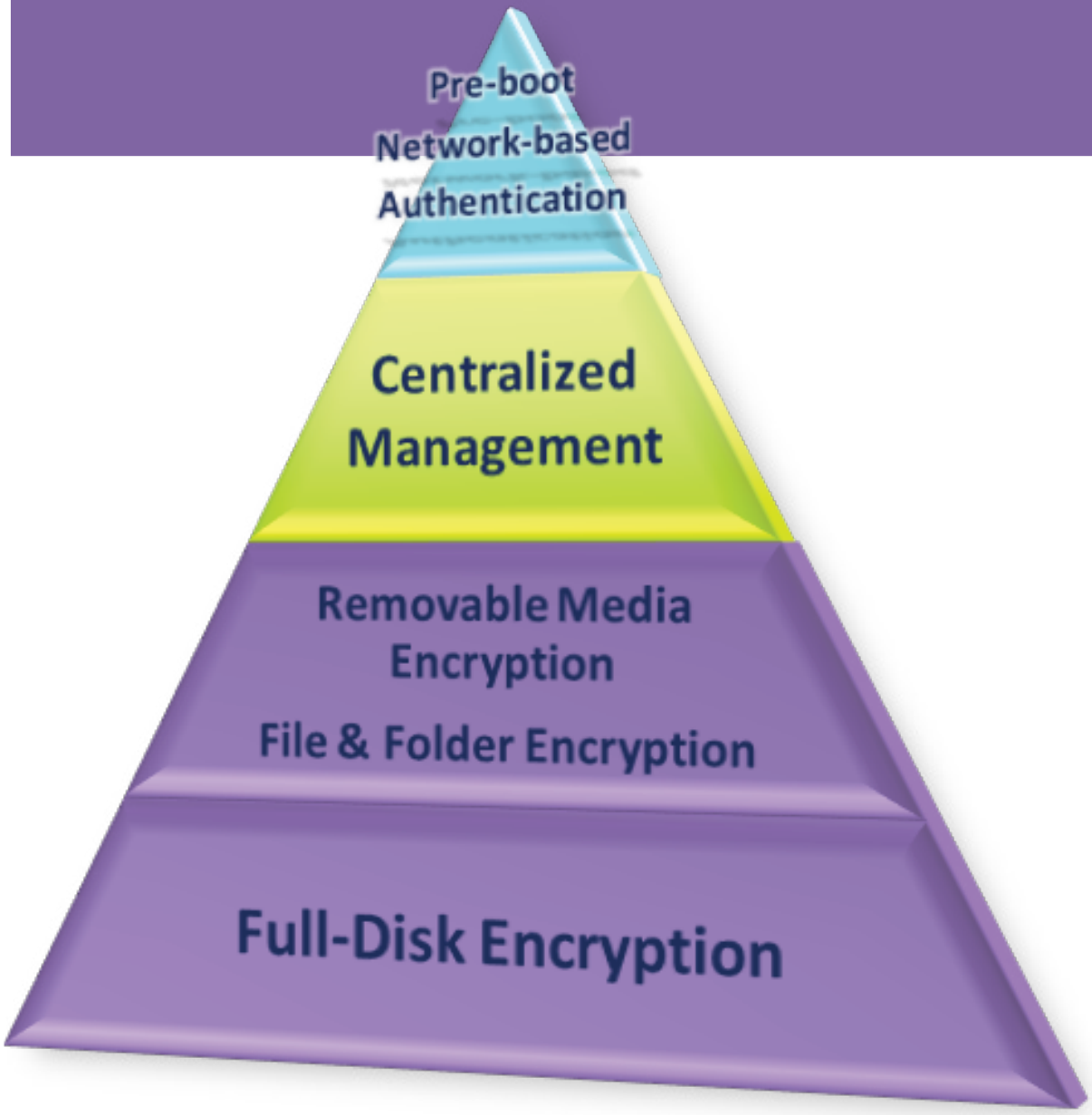
DATA ENCRYPTION DEFINED

Data encryption refers to the process of transforming electronic information into a coded form that can only be read by those authorized to access it. To read an encrypted file, a user must have access to a secret key or password that enables them to decrypt it.

The way in which an organization can protect their data encompass a variety of options. The foundation or core group of options typically start with:

- **Full Disk Encryption (FDE)**: Protects the entire hard disk (all sectors and volumes) and can only be accessed with a secure key
- **Removable Media Encryption (RME)**: The protection of all or a portion of a USB key, external hard drive, or similar removable media.
- **File and Folder Encryption (FFE)**: Protection is associated with specific folder or files where they are encrypted with specific user access permissions, much like network permissions.

There are a number of solutions available to fulfill virtually any data protection requirement, so before embarking on any new project, it's important to research and understand the options that work best for your unique situation.



BENEFITS OF DATA ENCRYPTION

The US Privacy Act, PIPEDA, FERPA, and the Data Protection Acts of the United Kingdom and European Union have all defined the way that data can be used and the penalties for its mishandling.

Data encryption has several advantages that enable educational institutions to comprehensively protect and secure data.

REGULATORY COMPLIANCE

- Data encryption enables organizations to better adhere to numerous local, state, federal and global privacy laws and regulations.

DATA SECURITY

- Encrypting data provides protection for sensitive information whether it's stored on a desktop or laptop, a smartphone, tablet, removable storage media, an email server or even the network, so in the event the device is lost or stolen, the information is protected.

TRANSPARENCY

- Data encryption solutions enable businesses to run at their normal pace while the encryption solution silently secures critical data in the background. Some of the best data encryption options perform without the user even being aware.

PEACE OF MIND

- Despite best efforts, data breaches can occur. Laptops and removable storage devices are prone to theft and loss. Data encryption protects critical assets if it falls into the wrong hands, and protects the integrity and credibility of your organization.
- The use of encryption provides a "safe harbor" in the event of a data breach.

DEBUNKING DATA ENCRYPTION MYTHS

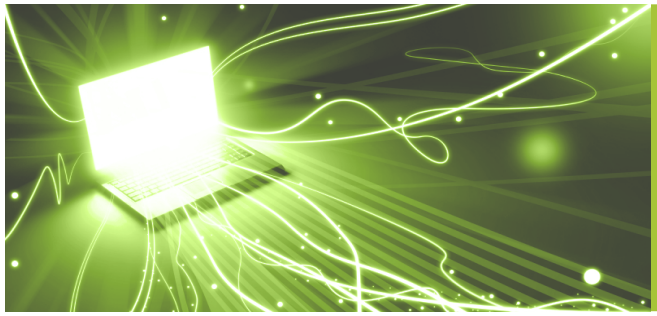
Despite the obvious benefits of protecting your data using an encryption solution, you might have heard comments like,

"Why do we need all this security, we've got strong passwords. " Or, "Data encryption - that's going to put a massive strain on the IT department".

Unfortunately, these common misconceptions surrounding encryption are based on a misunderstanding of the technology or on outdated concepts. They persist, even among those who are generally knowledgeable about computers. These myths sometimes cause decision makers and IT groups to argue against data encryption, or to dismiss the technology altogether.

By understanding how to address these misconceptions, you'll be well armed when building the business case for data encryption. While this eBook addresses some main points, WinMagic's white paper **Demystifying Data Encryption** really digs into the issues and provides an insightful look at the solutions and strategies that dispel them.

KEY MISCONCEPTIONS ABOUT DATA ENCRYPTION



1 DATA ENCRYPTION IS A MAJOR HEADACHE FOR THE USER AND IT

When computer processors were less powerful, data encryption significantly slowed system performance. As a result, data encryption was established in many peoples' minds as a technology that caused poor performance. But fast forward a few years and encryption operations are performed silently and efficiently in the background - even in mobile devices. Today, IT professionals advocate the universal use of encryption on all computing devices within an organization.

> Most users on modern systems don't even notice that encryption is taking place

Most agree that these solutions must be implemented in a way that can be managed and monitored consistently via central administrative management tools that deploy and maintain the encryption software transparently, with minimal impact on users. Individual solutions should be compared on a point-by-point basis to see how they measure up.

2 THERE IS NO COMPELLING REASON FOR ENCRYPTING PERSONAL OR CORPORATE DATA.

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

- Meeting regulations that apply to the protection of private individual data.
- Preventing unauthorized 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.

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

3 OS-BASED ENCRYPTION PROTECTION IS SUFFICIENT FOR ENTERPRISES

Encryption capabilities available through operating systems (OS), like Microsoft's BitLocker, 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 encryption solutions. As we'll see later via WinMagic's TCO calculator, the purchase price of a third party encryption solution is almost negligible when considering the total cost of ownership.

> OS-based encryption isn't FREE, the administration costs to manage it are very real

KEY MISCONCEPTIONS ABOUT DATA ENCRYPTION

4 COMPREHENSIVE ENCRYPTION SOLUTIONS FOR ENTERPRISES 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 a study released by the **Ponemon Institute**, it was determined that the least significant aspect of the loss was the actual cost of replacing the laptop.

> Factor in the true costs rather than simply the cost of the hardware itself

The results of the financial loss assessments were astounding and included the following 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 organizations surveyed, 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.

Furthermore, data breaches can cause long-term, if not irreparable damage to an organization's reputation. In one example, a data breach at an American University exposed 31,000 names, health records, financial data and social security numbers! The upshot? Not only was this breach an embarrassment to the school, but something that severely impacted the confidence in the integrity of the institution.

TOTAL COST OF OWNERSHIP EDUCATORS

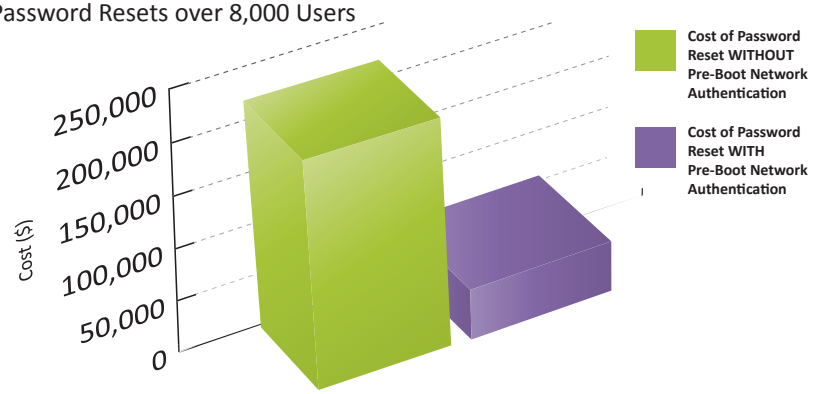
The challenge with data security solutions for most organizations is trying to balance the expense of the solution against the productivity of the users. Maximizing that total cost of ownership (TCO) of the solution is critical.

A recent study from the **Ponemon Institute** looked into what an encryption solution would cost an average organization per year. The results were shocking. What became apparent was that with features like pre-boot network authentication (WinMagic's PBConnex), data encryption solutions could help reduce TCO by not only managing encryption and security but improving the efficiency of other processes for IT Administrators such as support.

Looking at typical costs associated with Password resets and device staging alone, the savings were staggering.

Cost Savings with Pre-Boot Network Authentication

Password Resets over 8,000 Users



PASSWORD RESET - SAVINGS

Times per user per annum	3.3
Value of Tech and User Time for reset	$8.10
Total cost of password reset for user/tech per annum	$26.70
Savings with Pre-Boot Network Authentication	$20.04
Total Cost Saving in Password resets per organization of 5,000 devices	$100,200

STAGING AN FDE COMPUTER - SAVINGS

Time to stage a computer with FDE	20 mins per machine
Time to stage computer using Pre-Boot Network Authentication	5 mins per machine
Value of Tech time to stage machine	$12.00
Value Saved with Pre-Boot Network Authentication	$9.00
Size of Organization	5,000
Total Cost Saving to stage a computer per organization	$45,000

WHAT TO LOOK FOR IN A BEST-IN-CLASS DATA ENCRYPTION PROVIDER

Before embarking on a data encryption initiative, you'll need to determine which provider can offer you the protection that best suits your needs. Obviously, there's a lot to think about, but by taking the time to select the right provider, you'll be poised for success as you move forward with your deployment. These are some key things to look for when seeking out a 'best-in-class' data encryption solution.

1 INTEGRATION

Look for a provider that has proven third party integration with hardware and software companies for optimal security offerings and increased functionality. Be sure they offer services for different operating systems and hardware, and mobile device management for devices like tablets and smart phones.

2 PRE-BOOT NETWORK BASED AUTHENTICATION

Pre-boot network authentication (wired or wireless) utilizes network based resources to authenticate users, enforce access controls, and manage end point devices before the operating system loads.

This approach to FDE management also results in significant cost savings for organizations by streamlining the time and cost associated with things such as password resets and device staging. This capability truly separates the best from the rest.

3 BYOD READY: MULTI-PLATFORM/ MULTI DEVICE MANAGEMENT

With 76 percent of employees today using more than one mobile device, BYOD is virtually everywhere. Add to that, many schools employ a mixture of old and new systems. Ensure the provider you select can offer central management for systems running any operating system, whether it's Windows, Mac OS X or variants of Linux, Android, iOS. Mobile device management offers the 'proof' that IT administrators require to ensure compliance with key industry regulations while at the same time offering a strong solution for BYOD environments.

WHAT TO LOOK FOR IN A BEST-IN-CLASS DATA ENCRYPTION PROVIDER

4 SINGLE MANAGEMENT CONSOLE

Monitoring and tracking devices from a single console reduces reliance on IT and enables easy integration into accounts with laptops, desktops, tablets, smart phones, and SED devices and supports full mobile device management. A central view of all devices reduces the need for desk side support calls because administrators can determine if a device is in a secure, compliant state, and if not, quickly contact the user to rectify the situation.

5 SUPPORT FOR SELF ENCRYPTING DRIVES (SEDS)

While SED technology has improved the security of laptops and workstations, it does not require specific authentication during boot up, leaving data at risk. Providers on your short list should have the capability to centrally support users with SED devices and employ a pre boot authentication to ensure the drive is encrypted, compliant and functioning properly, while taking advantage of the transparency, performance and security that a SED offers.

6 FILEVAULT MANAGEMENT OR FULL DISK ENCRYPTION FOR MAC OS

Some organizations prefer to leverage the native encryption and security offered by Mac OS X's FileVault 2. Using a solution that supports FileVault 2 and offers centralized management to oversee all devices ensures you've got the best of both worlds.

WINMAGIC®
DATA SECURITY

WE'LL PROTECT YOU...

WinMagic understands the data security challenges and changing needs of higher education institutions. In order to help effectively meet and adapt to the changing needs and expectations of all their constituents, WinMagic works closely with a wide variety of colleges and universities, standard bodies, higher education associations, and education industry leaders to develop and deliver the most secure data encryption protection.

> "We have been very happy with performance of SecureDoc™. It has met all our data protection requirements without inconveniencing faculty and staff, and I would definitely recommend it to other organizations."

D. Douglas Badger, CGA CISA CGEIT
Director, IT Portfolio Management & Systems Assurance,
Office of the CIO, University of Guelph

SECUREDOC™ 6.1

SecureDoc is a comprehensive disk encryption and data security solution that secures data at rest. It has two main components: the client software used to encrypt and protect data and the server software (SecureDoc Enterprise Server or SES) used to configure, deploy, and manage encryption for an entire organization.

Armed with a full arsenal of data protection solutions, SecureDoc provides: full disk encryption; PBConnex Pre Boot Networking, file and folder encryption; removable media and removable media container encryption; departmental server encryption; centralized management; Active Directory and LDAP integration; Mobile Device Management (MDM) and much more. SecureDoc also makes it easy to centrally manage and use standard drives and self-encrypting drives including TCG OPAL-compliant drives.

SecureDoc protects sensitive data stored on desktops, servers as well as portable media such as laptops and removable media including USB thumb drives and CD/DVDs. It is compatible with all editions of Microsoft Windows 7, Vista, XP, and 2000 as well as Mac OS X Mountain Lion, Lion, Snow Leopard, Leopard and Linux platforms.Our software can help organizations meet internal requirements and government or other regulations to maintain the security and integrity of your data.

WINMAGIC®
DATA SECURITY

PBCONNEX™

SecureDoc with PBConnex is the only data encryption and management solution that allows for pre-boot network authentication either wired or wirelessly. PBConnex utilizes network based resources to authenticate users, enforce access controls, and manage end point devices before the operating system loads. This unique and ground-breaking approach to FDE management also results in significant cost savings for organizations by streamlining the time and cost associated with things such as password resets and device staging. In addition, multiple users can safely use the same device without ever putting confidential data at risk.

SES WEB CONSOLE

The SES web console provides a web-based interface for SecureDoc Enterprise Server, WinMagic's solution for centrally managing encrypted devices in an enterprise environment. The SES web console supports many of the daily administration features provided by the SecureDoc Enterprise Server, including user management, administrator management, device management and recovery, password management, and report management. It also includes a Mobile Device Management (MDM) server component.

MOBILE DEVICE MANAGEMENT (MDM)

SecureDoc's MDM feature is a key component of the SES Web console, offering enterprise customers a holistic view to their status of their mobile devices, allowing them to manage the deployment of Android® and iOS® devices and also to ensure that the appropriate security and password policies are enforced. SecureDoc MDM offers the 'proof' that IT administrators require to ensure compliance with key industry regulations while at the same time offering a strong solution for BYOD environments.

FILEVAULT 2 SUPPORT

SecureDoc offers one of the strongest Mac OS X FDE solutions available on the market today. For customers that prefer to leverage the native encryption and security offered by Mac OS X's FileVault 2 solution, SecureDoc can manage that as well. FileVault 2 enterprise management gives businesses the flexibility to choose how they want to encrypt and manage their Apple devices yes still have the ability to have all their devices managed by SES's central management console.

READY TO LEARN MORE?

WinMagic provides the world's most secure, manageable and easy-to-use data encryption solutions. With a full complement of professional and customer services, WinMagic supports over five million SecureDoc users in approximately 84 countries. We can protect you too.

For more information on SecureDoc Enterprise Server contact **sales@winmagic.com** or visit our website to access a number of valuable resources:

PRODUCT PAGE
http://www.winmagic.com/products

WHITE PAPERS
http://www.winmagic.com/resource-centre/white-papers

CONTACT

WinMagic Inc.
Phone: 905. 502. 7000
Fax: 905. 502. 7001

Toll Free: 888. 879. 5879

sales@winmagic.com
www.winmagic.com

SOCIAL MEDIA


http://blog.winmagic.com/


http://www.facebook.com/WinMagicInc


http://www.linkedin.com/company/winmagic


http://twitter.com/winmagic

http://www.youtube.com/user/winmagicinc

WANT TO TRY OUR SOFTWARE?

CLICK HERE TO REQUEST A FREE EVALUATION >