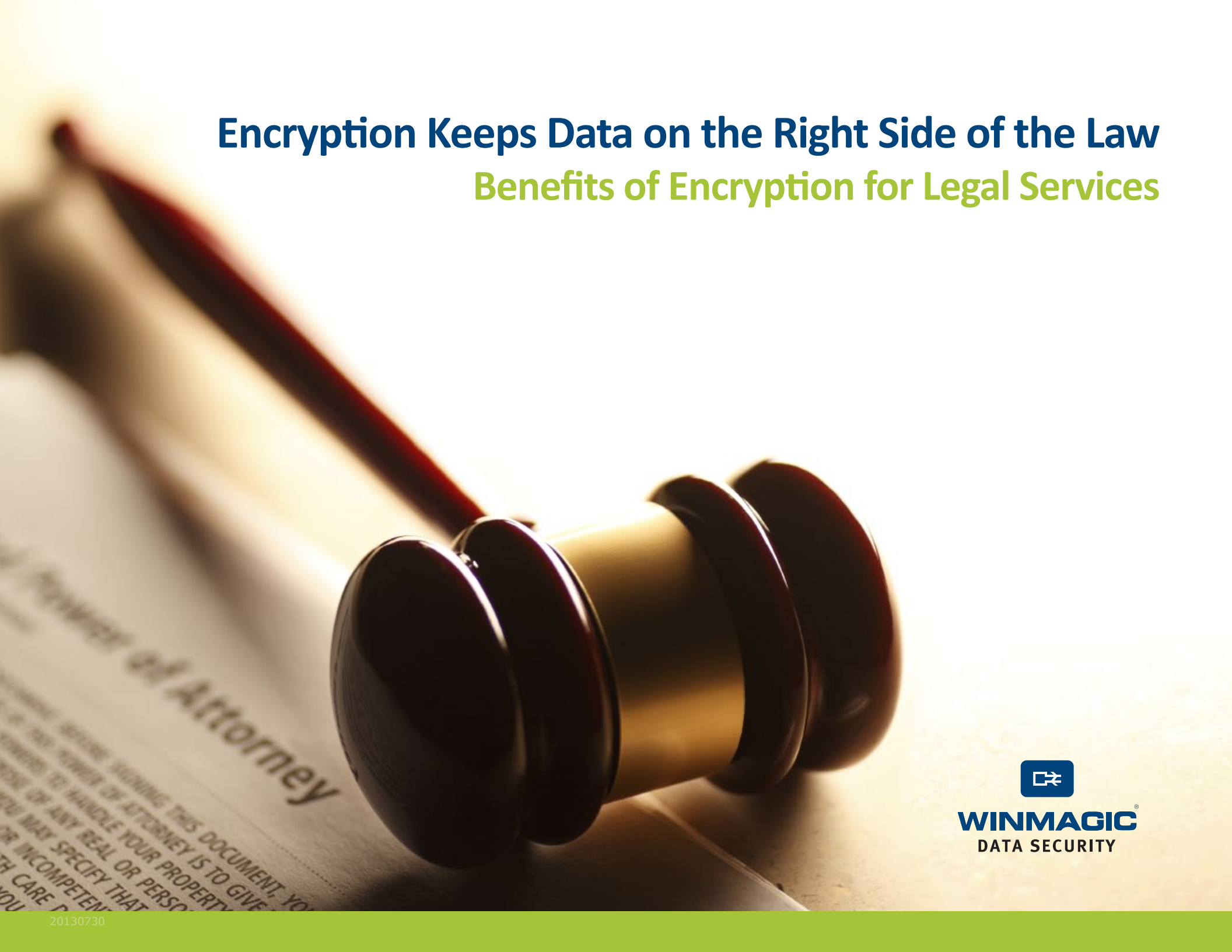


Encryption Keeps Data on the Right Side of the Law

Benefits of Encryption for Legal Services



WINMAGIC®
DATA SECURITY

FOREWORD

Email, content management systems, e-discovery tools and the increase use of mobile devices enables law firms and legal offices to be more nimble and efficient and to deliver better service to their clients. Meanwhile, many organizations in the legal services field still rely on CD-ROMs and USB drives to share files that contain crucial evidence, case proceedings and detailed information about clients and witnesses between staff or other organizations such as other law offices or the courthouse. All of these tools and storage media increase the chance of information being misappropriated as new access points for data proliferate. Sensitive information that fall into the wrong hands can influence the outcome of a trial, expose the firm to risk and liability and even threaten someone's personal safety.

As a result, many law firms have begun to look to data encryption to safeguard their communications and corporate assets from unauthorized access.



WINMAGIC®
DATA SECURITY

TABLE OF CONTENTS

FOREWORD	1
WHY YOU SHOULD EMBRACE ENCRYPTION	2
FINDING THE IDEAL ENCRYPTION	3
READY TO LEARN MORE?	4

WHY YOU SHOULD EMBRACE ENCRYPTION



PAPER TRAILS

Good encryption software not only secures data at rest; it can also provide proof that a device was in a secure state when it was lost or stolen, preventing unauthorized access and limiting potential risk relating to chain of custody for information.



LIABILITY REDUCTION

In many jurisdictions, organizations are required to report a security breach to clients or even the public. A paper trail through data encryption can in turn protect a firm from liability in the event of a breach caused by circumstances out of their control or behavior of a third party.



ENSURES COMPLIANCE

Encryption can help firms comply with the regulations of regional bar associations as well as the regulatory environments of clients (i.e. HIPAA for healthcare clients).



IDENTITY THEFT PROTECTION

Encrypting devices safeguards the identities of staff, clients, witnesses and anyone connected to a case if a device is misplaced or stolen.



BRANCH OFFICE DATA PROTECTION

Many firms have multiple branch offices of varying sizes across the country or around the world that may be at risk of break-ins and theft. If a location does not have on-site IT staff, an encryption solution with centralized management capabilities can manage and protect data stored at all locations.



COMPETITIVE EDGE

Depending on the type of law being practiced by the firm as well as the clients being served, being able to demonstrate a secure and well-managed environment with a sound encryption strategy will appeal to potential customers.



LOWER TOTAL COST OF IT OWNERSHIP

In the event of a breach or lost or stolen devices, an encryption strategy can help realize potential savings of up to 20 times your IT Cost of Ownership.



BRING YOUR OWN DEVICE (BYOD) SUPPORT

Whether a firm is already allowing staff to use their own mobile devices or are considering smartphones or tablets as part of standard business operations, encryption can secure data on devices and enforce policies at the user level to ensure all information is safeguarded.

FINDING THE IDEAL ENCRYPTION

There are several things you should consider when implementing encryption technology:

EASE OF USE

Whether it's encryption for laptops, desktops, mobile devices or removable media storage, it should be simple and non-intrusive for the user. IT administrators should rarely have to consult a help file, and documentation should be clear and easy to understand. Encryption should also be transparent to end users so they can carry on their normal activities without affecting performance or even realizing encryption is running in the background.

FUTURE PROOFING

Look for a solution and a vendor that can grow with the organization's requirements. If initial deployment is focused on securing office-based computers but there are plans to address BYOD down the road, engaging a single vendor is better than implementing a variety of point solutions over time.

DON'T OVERBUY

Most users and organizations need only a few features to meet their encryption requirements; having more bells and whistles than necessary will only frustrate and confuse users and exhaust IT budgets for features that will never be used.

CROSS-PLATFORM

An encryption solution should be able to address all of the systems, devices and files employed by the firm. Look for an encryption vendor that has strategic partnerships with storage media vendors, device manufacturers, and commonly used operating systems and software suites. They should be able to encrypt any file.

COMPLIANCE

Look for a vendor who not only understands the latest trends in encryption technology but also the regulatory and compliance requirements for any jurisdiction where law is being practiced by the firm, as well as those that affect the firm's customers.



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>

WANT TO TRY OUR SOFTWARE?

CLICK HERE TO REQUEST A FREE EVALUATION >

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>