ENCRYPTION FOR MOBILE AND CLOUD COMPUTING

Keep data safe, even as it moves outside the perimeter of the traditional network.

Executive Summary

As organizations increase their use of mobility and cloud computing, they're finding it more complex than ever to create an effective security strategy and protect sensitive data. Users demand access to data no matter where it is, as new technologies expand the perimeter of the enterprise network. Organizations strive to keep this data out of the wrong hands, but the challenge to protect it is growing.

To address this challenge, organizations are employing storage encryption, which can be implemented at the disk level or at the file level. IT departments implement full-disk encryption (FDE) to scramble the contents of an entire physical disk. FDE protects data on a device until a user or administrator provides successful authentication. Alternatively, file encryption can safeguard data in individual files, decrypting the file and making it available for access and editing when a user authenticates his or her identity. The effective use of file encryption can prevent data breaches and help organizations achieve compliance with various laws and regulations.

Table of Contents

SHARE THIS WHITE PAPER

The Situation: Why Encryption Is Necessary

The days of having all enterprise data inside a strictly defined perimeter are long gone. Indeed, data travels just about everywhere today. The rise of mobility has resulted in the extensive sprawl of enterprise data. Many organizations allow sensitive data to be stored on mobile devices, such as smartphones and tablets. This creates new challenges in safeguarding this data, particularly because network security controls may not extend to mobile devices.

To further complicate today's security picture, consider the challenges posed by cloud computing. Data is no longer confined to a particular physical server; rather, it moves from server to server, sometimes data center to data center. With public and hybrid clouds, an organization's data is not necessarily under its direct control. Instead, the cloud provider may be responsible for various security controls.

Whether mobile technologies or cloud technologies are a concern for an organization, the same fundamental issue is relevant: addressing the organization's loss of control over sensitive data in an environment in which users increasingly demand access to data at any time on any device. A single data breach, in which an attacker gains unauthorized access to an organization's sensitive data, can mean millions of dollars in direct financial damages, not to mention serious harm to the organization's reputation.

Increasingly, organizations are turning toward storage encryption solutions to protect their sensitive mobile and cloud-based data. Storage encryption can prevent a variety of attacks from succeeding and is becoming widely recognized as a preferred form of data security for mobile and cloud environments.

COMPLIANCE CHALLENGES

Most organizations have sensitive data that is subject to some form of regulation, such as the Health Insurance Portability and Accountability Act, the Health IT for Economic and Clinical Health Act, the Gramm-Leach-Bliley Act and the Payment Card Industry Data Security Standard. These regulations require certain types of sensitive data, such as medical and financial records, to be protected in order to prevent data breaches.

Failure to adhere to these initiatives can be costly, particularly if a data breach occurs. Penalties for such breaches can exceed $1 million. Therefore, organizations must take the threat of data breaches and compliance violations seriously by ensuring that sensitive data is properly safeguarded, particularly in mobile or cloud environments. Encryption doesn't provide an unbreakable defense against these threats, but it does put safeguards in place to show that an organization its making its best effort to protect data.

How Encryption Works

Encryption is the process of converting an original source (also known as a plaintext) to a scrambled form (known as a ciphertext), so that the plaintext cannot be readily recovered from the ciphertext without knowledge of a secret value (stored in the form of a cryptographic key). The method used to conduct the scrambling (encryption) and unscrambling (decryption) is known as a cryptographic algorithm, and the security of the ciphertext does *not* depend on the secrecy of the algorithm. In fact, the most trusted algorithms are those that have been publicly vetted to find weaknesses.

The generally accepted gold standard for encryption today is the Advanced Encryption Standard (AES), which requires a cryptographic key length of 128 bits. However, computing technologies are rapidly growing in their capabilities to guess shorter keys using brute force, so many in the security industry are moving to 256-bit AES keys to protect against future threats. The only downside to using a longer key is that encryption and decryption activities require greater processing resources. But in most environments, this creates only a negligible delay at worst.

Encryption can be applied to data at rest (stored data) and data in motion (transmitted data) to protect it from a variety of threats. Both data at rest and data in motion need protection via encryption in cloud and mobile environments. This can be accomplished through a virtual private network, Transport Layer Security–wrapped HTTP or other means. Ultimately, the intention of encryption is to prevent the unauthorized use of information even when someone gains unauthorized access to it.

Data at rest is protected through storage encryption — the application of encryption techniques to stored data. Several forms of storage encryption exist, but the two most relevant for cloud and mobile environments are full-disk encryption and file encryption. As the name implies, FDE is literally the encryption of the entire physical disk. FDE is enforced when a device is not booted, so it protects all data on a device until a user or administrator provides successful authentication. At that point, FDE decrypts the drive so that it can be booted and used.

File encryption involves the encryption of individual files, such as user documents. File encryption is enforced at all times except when an individual file is being used. After a user authenticates his or her identity to the file encryption software, the software decrypts the file and makes it available for access, editing, etc. When the user is done with the file, the software re-encrypts it.

With both FDE and file encryption, managing the relevant secret cryptographic key represents a major challenge. The key must be safeguarded so that only authorized personnel have access to it (and therefore the ability to undo the encryption). An organization should maintain ownership of its encryption keys and store them separately from the encrypted data. If the keys and encrypted data are stored together, a single attack can recover both the encrypted data and the key protecting it.

Encryption and Cloud Computing

In cloud environments, maintaining the security of sensitive data and achieving compliance with laws and regulations for protecting that data are both of utmost importance. However, laws and regulations generally list only the minimum controls required and do not always cover generally recommended practices for security. Also, many laws and regulations prescribe the use of general controls, such as encryption, without specifying which forms of encryption are effective and acceptable. Therefore, organizations must understand the relationship between encryption and cloud computing when planning cloud security controls.

The requirements for encrypting sensitive data in the cloud are generally the same for public, private or hybrid clouds. The only difference is that in a private cloud, the cloud provider and the cloud customer are generally (but not always) the same organization. Storage encryption can be applied by the cloud provider (provider-side encryption), the customer organization (client-side encryption) or both. It is generally recommended to allow the cloud provider to control FDE, since the provider maintains physical control over the cloud servers. FDE protects data at rest when the server is not booted, such as when the server is being physically moved from one data center to another, or when a server hard drive is being sent to a manufacturer for repair. When the servers are up and running, which is most of the time, FDE is irrelevant.

Customers sometimes grant a cloud provider administrative privileges to maintain file encryption; however, this is not a recommended practice. Doing so gives the cloud provider control over the encryption keys, reducing accountability and increasing the chance of an insider attack or other compromise of the encrypted data. It is generally safer for a customer to maintain control of its own keys and to store these keys separately from the encrypted data — for example, locally storing the keys used to encrypt cloud-based files.

75%

Percentage of organizations that are using, or plan to use, mobile device or application management technologies to protect their mobile devices and data against cyberthreats

By following these practices, a cloud customer can ensure that a single compromise will rarely lead to the exposure of encrypted files (unless those files happen to be in use at the time that the compromise occurs). Every organization with sensitive data stored in the cloud should use file encryption to protect it. Organizations also must ensure that their sensitive data is protected in transit, including when cloud workloads are automatically migrated from one physical server to another. File encryption does provide protection for this migration, and some forms of file encryption remain in effect with a file no matter where it is transferred, thus eliminating the need for separate encryption when that data is in motion.

Encryption and Mobility

Mobile environments have a lot in common with cloud environments when it comes to storage encryption. Sensitive data on mobile devices should primarily be protected using file encryption. This supports the confidentiality of sensitive data even if a mobile device is lost or stolen, assuming that other security practices for mobile devices are followed (for example, devices should be configured to lock themselves after a period of inactivity and to require a personal identification number to regain access).

Mobile devices typically do not have built-in file encryption capabilities, so achieving file encryption requires adding software to the mobile device. Fortunately, many enterprises already have deployed products with file encryption capabilities on their mobile devices, such as mobile device management. MDM technologies can manage a wide range of security controls on a mobile device, including the encryption of sensitive files. What's more, MDM technologies are supported not only on organization-controlled mobile devices, but also on personally owned smartphones and tablets that may be part of a bring-your-own-device program. Enterprises that already have MDM technologies should carefully evaluate their storage encryption capabilities and use them to ensure that sensitive data on mobile devices is encrypted using file-level encryption.

Mobile content management is another category of products that include encryption capabilities for sensitive mobile data. An MCM product provides centralized collaboration for mobile users, but with security applied, so that sensitive data being used collaboratively is encrypted both at rest and in motion. With most MCM products, sensitive data is stored centrally, such as within a public cloud — not on the mobile device itself. MCM products can securely download a sensitive file to a mobile device and even protect that file's data while in use, then securely transfer the file after use back to the secure centralized storage system.

An organization with major security concerns could leverage both MDM and MCM solutions for its mobile devices. The MCM solution would safeguard collaborative data, while the MDM solution would secure locally generated and stored data.

CDW: A Security Partner That Gets IT

As a leading provider of technology solutions, CDW can help you leverage cloud computing and mobility securely through use of encryption technologies.

CDW offers dedicated account managers who are responsible for helping you choose the best IT products and services to meet your needs, including customized solutions. CDW also offers an experienced team of security solution architects who are specifically focused on ensuring that your security solutions are properly designed and implemented.

The CDW approach includes:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future environment design and proof of concept
- Procurement, configuration and deployment of the final solution
- Ongoing product lifecycle support

To learn more about CDW's cloud and mobile encryption solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/security.

Symantec

Symantec™ Enterprise Solution provides multiple layers of protection to deliver strong data protection for mobile, endpoints and mail/web infrastructure. It includes products protecting against malware, data loss and spam threats with endpoint security, drive encryption and system recovery.

cdw.com/symantec

KASPERSKY lab

Kaspersky® provides a complete, fully integrated platform that combines anti-malware protection, robust application, device and web control tools, plus systems and patch management, data encryption, and Mobile Device Management — all managed from a single console and available for a single cost. This is not simply a collection of solutions strung together and sold as a "suite." It's a unified platform that makes it easy for you to see your risk across all your systems and endpoints, apply your policies consistently, and bring your security posture in line with your objectives.

cdw.com/kaspersky

SafeNet

Securing data over its lifecycle, from the data center to the cloud becomes more important by the day. SafeNet® encryption solutions deliver robust coverage — securing databases, applications, personal identifiable information (PII), and storage in the physical and virtual data center and the cloud. Moreover, SafeNet also provides the critical key management needed to effectively and efficiently enable protection across the enterprise wherever data resides.

CDW.com

SHARE THIS WHITE PAPER

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.
All other trademarks and registered trademarks are the sole property of their respective owners.
Together we strive for perfection. ISO 9001:2000 certified

CDW PEOPLE WHO GET IT™