

# **Protecting Data at Rest**

## What to Consider When Selecting a Solution for Disk, Removable Media, and File Encryption



## OVERVIEW

Data is one of the most important assets within organizations, second perhaps only to employees. As incentives for malicious attacks continue to grow, the consequences of data compromises are rising accordingly. Additionally, organizations face complex challenges regarding the need to achieve an effective balance between risk of exposure and legitimate, easy access to data across the enterprise.

Full-disk, removable media, and file/folder encryption provide extensive protections against accidental loss and malicious acts, with broad coverage ranging from laptops to enterprise application servers to USB thumb drives. Combined, the approaches ensure maximum security for sensitive data at rest, and even offer protection for data in motion over private and public networks.

The ideal data at rest encryption solution also permits users to access the data they need in ways that are familiar and comfortable, without loss of performance, and with all security-related processes running transparently in the background. Furthermore, a well-designed, consolidated security management platform can simplify administrative tasks, lower costs, provide easy, non-disruptive deployment and maintenance, and efficiently support all compliance needs.

As internal security threats continue to grow in number (currently estimated at 75% of all security risks), the combination of disk, removable media, and file encryption provides vital data protection that strengthens security without interfering with critical business processes, end-user behavior, and ongoing IT operations.

## APPROACHES TO DATA AT REST PROTECTION

There are two distinct and complementary approaches to data at rest protection: full disk encryption (“power off” encryption), and file encryption (“power on” encryption). The most comprehensive data at rest protection solutions include both of these methods.

### Full disk and removable media encryption

Full disk encryption methodologies encrypt all data on a disk partition, which includes everything but the master boot record and a small pre-boot operating system. This means that the operating system files, swap files — and even data which has been “deleted” but actually still remains on the machine — are all encrypted. The first step is an initial encryption of the entire partition and/or full disk, after which the subsequent encryption and decryption process occurs on the fly. Full disk encryption occurs at a very low level in the operating system. Successful user authentication must occur before decryption of the Windows operating system begins. Ideally, protections should be transparent and fast, so end users are unaware that encryption/decryption processes are functioning in the background.

### File encryption

File encryption allows the contents of files and folders to be encrypted. Encryption at this level protects data stored locally or remotely. Furthermore, since network share files, when transmitted to a client machine, are not decrypted until they have arrived at their destination,

*The ideal data at rest encryption solution also permits users to access the data they need in ways that are familiar and comfortable, without loss of performance, and with all security-related processes running transparently in the background.*

*Full disk encryption methodologies encrypt all data on a disk partition or removable media. File encryption allows the contents of files and folders to be encrypted.*

strong file encryption also ensures that data in motion, traversing a network, remains secure.

File encryption prevents users without appropriate authorizations from decrypting certain types of information — for example, personnel records that contain Social Security numbers, salary data, and other personally identifiable information (PII) — even if they are able to gain access to the machines themselves. One major advantage of file encryption is that it enables IT staff to service equipment in a power-on state without allowing them access to sensitive data.

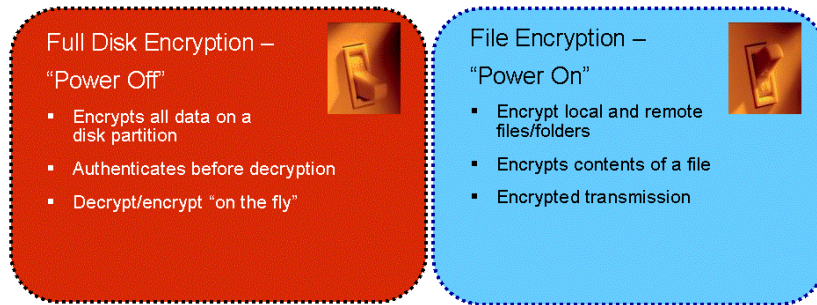


Figure 1: Data protection approaches

## MAJOR THREATS TO SENSITIVE DATA

Common threats to sensitive data include loss or theft of data device, improper storage or disposal of equipment, malicious acts from within the organization, and specific software and hardware vulnerabilities.


### Loss or theft of data assets

Devices at risk for loss and theft include: computers, such as laptops, workstations, and servers; removable media such as USB flash drives and hard disk drives; CDs, and DVDs; as well as mobile devices such as smartphones and PDAs. Encrypting sensitive data, or encrypting all of the data on particular device, reduces the risk associated with theft or loss. Typically, data privacy regulations require reporting of such incidents; however this is usually not the case if the organization can demonstrate that the drives and removable media in question were encrypted.

### Improper storage or disposal of media

Leased, rented and end-of-life equipment can become high security risks. In a MIT study, researchers purchased 158 disk drives online and from computer stores, computer salvagers, and swap meets. Upon investigation, they discovered that 74 percent of the machines (117) contained old data that could be recovered and read. Seventeen percent (28) contained fully installed and functional operating systems with user data that required no effort to recover. Thirty-six percent of the machines (57) had been freshly formatted, but still contained old data that was very easily recovered. Only 9 percent (12) of the drives had been properly sanitized before being put up for sale. The remaining 29 drives were non-functioning, yet a mechanical repair of the drives might have made it possible to recover data from those as well.

*Encrypting the entire contents of a hard drive thwarts attacks that use boot disks to bypass the built in security of the OS. Even if an attacker gets past OS controls, the data remains encrypted.*



The data found on these machines also revealed strong security implications. Financial log files on one drive yielded what appeared to be 3,000 credit card numbers and bank account numbers, with detailed transaction dates and account balances. Another drive that had been reformatted, but was still recoverable, contained nearly 4,000 credit card numbers. The researchers speculated that these hard drives may have come out of ATM machines.

This study confirms that improper disposal of computing equipment poses significant security risks. Full disk encryption is the most effective way to significantly reduce this risk, because even if sensitive data remains on the drive it remains secure.

#### **Internal threats**

Internal security threats include misuse of accounts or privilege escalation, weak or improper file permissions, abuse of administrative privileges, and placing sensitive data on insecure media. These risks can be mitigated by encrypting sensitive files at a departmental or organizational level, which ensures the confidentiality of the information while allowing administrators to continue to perform their typical duties. For example, administrators can manage folders and folder permissions and do backups, but without the proper authentication they are unable to decipher the files that are actually encrypted within those folders. A common case in point is sensitive Human Resources data that are stored on a HR server. With proper file/folder encryption, even IT administrators could not access such data unless they were also a member of the HR group with the associated privileges.

#### **Exploitation of vulnerabilities**

Without strong encryption, boot disks that allow attackers to bypass OS security pose additional risks. Examples include live Linux boot-up disks or the ability to boot from a USB thumb drive.

Encrypting the entire contents of a hard drive, sector by sector, thwarts attacks that use boot disks to bypass the built-in security of the OS. Even if an attacker gets past OS controls, or attempts to overwrite the hard drive, the data remains encrypted and therefore worthless. For network attacks, file encryption provides appropriate protections. With file encryption, even if attackers were able to break into a network gain access to certain directories, they would not be able to decipher encrypted data.

## **PROTECTION FOR DATA AND DEVICES**

It is critical to properly identify the types of data and devices that require protection. Equipment protection should extend to all mobile devices and removable media, as well as computer ports. Vulnerable information includes confidential data, deleted files, backup data, and temporary files, with coverage necessary at both the application and the system level.

#### **Mobile devices and removable media**

Encrypting all data on mobile devices and removable media limits the risks associated with loss or theft, reducing concerns over what might or might not have been in certain folders or partitions on the drive. Complete rather than partial encryption eliminates guesswork and administrative costs.

### Confidential data

Confidential data frequently is owned by a single department within an organization. Personally identifiable information in confidential HR files is a common example. This data should be encrypted at the department level, so only authorized departmental users can gain access to it. Full disk encryption provides added protections, covering data at the application and system level and also protecting temporary and deleted files. The combination of full disk and file encryption ensures maximum safety.

### Other vulnerable data

A file that has been “deleted” from the hard drive is not really gone. Deletion simply erases the pointer to that file, which means that the data is still there and can be read unless it is encrypted. Backup data is also vulnerable and therefore needs to be encrypted when it is removed from the originating system, especially if it resides on media that can easily be transported. The data at rest solution should work smoothly with all existing backup systems and provide the ability to securely wipe files that should be permanently deleted.

## CRITERIA FOR SUCCESS

In order for a data at rest solution to be fully accepted by end users, and provide a practical security methodology for the enterprise as a whole, it must deliver three key attributes: **security, usability and manageability.**

If the security is inadequate, the solution is by definition useless. If end users push back because the solution is cumbersome, or slows down the performance of their machines, it undermines effectiveness and raises management costs. Finally, if the solution is difficult to deploy, then administrative concerns and costs may outweigh the security benefits.

A data at rest solution should provide maximum protection, offer ease of use to end users, and provide simplified management capabilities that ensure easy deployment and maintenance. Desirable administrative features include efficient and secure mechanisms for recovering data and emergency authentication in the case of lost or forgotten end-user smart cards and passwords. Equally important are strong reporting capabilities that simplify auditing and ensure organizations meet compliance requirements, are necessary.

*A data at rest solution should provide maximum protection, offer ease of use to end users, and provide simplified management capabilities that ensure easy deployment and maintenance.*

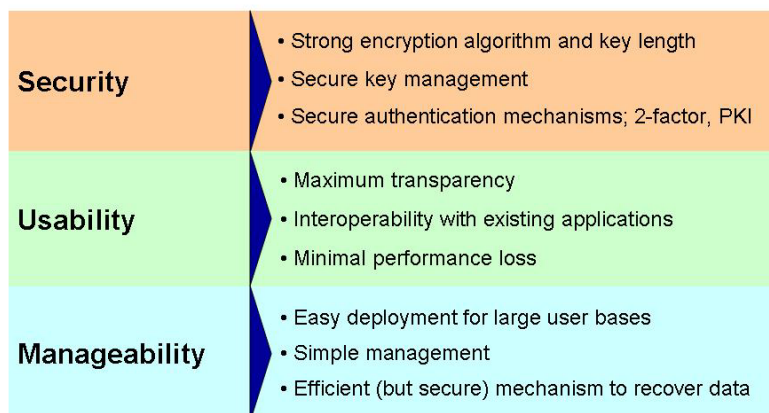


Figure 2: Key attributes of a data protection solution



## **Advanced security controls**

Major elements of a truly secure data encryption solution include: a strong encryption algorithm and robust key length; secure key management; strong authentication mechanisms such as two-factor authentication and PKI; and certification by recognized regulatory bodies.

Advanced cryptography: Encryption solutions are based on cryptography, and cryptography is only as strong as the algorithm and the length of the key used to encrypt the data. The standard in strong commercial cryptographic algorithms today is AES-256. However, depending on an organization's needs, other cryptographic algorithms can be used. Many effective, proven algorithms are available if AES fails to suit a particular organization's requirements.

Effective key management: Cryptographic keys need to be protected, but also must remain readily available to authorized users. Ideal key management solutions make it easy for only authorized administrators to securely generate, use and change keys, as well as archive them. Archived keys can be used for key recovery purposes and long-term data access—for example, if a user leaves an organization unexpectedly and administrators need to access the user's archived and encrypted information.

Certification: Certification is important in the encryption world in order to provide assurance of security claims and help meet compliance requirements. Examples include the internationally recognized Common Criteria certifications and FIPS 140-2 validation, which is assurance overseen by the U.S. Federal Government, regarding cryptographically-based security solutions. Many other regulatory agencies provide various levels of certification as well, targeting industries such as finance, healthcare and education.

Strong authentication: Strong authentication mechanisms—usually tokens or smartcards — are highly recommended for maximum data at rest protection. Public Key Infrastructure (PKI) is a preferred approach, but in organizations that have not yet deployed PKI solutions, password-only support should be available for non-token deployments.


## **Ease of use**

Disk encryption should enable users to go about their daily computer tasks in a way that is familiar, comfortable, and painless. If a security solution makes it difficult for users to do their work, they may find a way to get their work done by circumventing security controls. Desirable capabilities include non-disruptive deployment, background encryption/decryption processes, single sign-on (with credentials passed to the Windows OS upon login), negligible or no performance loss, and seamless interoperability with existing applications.

This transparency applies to removable media as well as conventional laptops, workstations, and servers. Data at rest protection solutions need to encrypt devices such as thumb drives, portable hard drives, or even CD-ROMs. They also should be able to identify "legitimate" removable media, and prevent the use of unauthorized media.

## **Simplified management**

Usability is critical for administrators as well as end users. A data at rest protection solution should not place undue burden on the IT management staff or on the helpdesk, and should enable implementation without extensive training.



Ease of use features: Required capabilities include: easy, transparent deployment across a large user base; centralized, simplified management, including single-point provisioning and de-provisioning, and efficient and secure mechanisms for data recovery.

Compatibility with existing resources: Proper data at rest solutions easily interface with existing user directories, such as Active Directory (so that access to encrypted data is tied to existing users/groups) and use existing administration tools. By using Active Directory – centric approach as opposed to proprietary management systems, one eliminates the potential for synchronization problems with redundant databases, and reduces security risks associated with the misconfiguration of users in these databases. Organizations that have built a disaster recovery system around their Active Directory infrastructure can leverage this capability, without adding cost or complexity.

In addition, many IT organizations use disk-imaging software to deploy and maintain critical enterprise systems. Data at rest solutions should work seamlessly with these tools. Since each environment is different, security solutions should be thoroughly tested in combination with these tools before deployment.


Also, companies should avoid disk and file encryption products that require a dedicated management server, which adds initial and ongoing costs that must be considered when determining the total cost of ownership for the data at rest encryption solution.

Individual accounts: Each user assigned to a mobile asset should be able to log in with his or her credentials. Some solutions, by contrast, require that users share a pre-boot account; that is, they share the same credential (e.g., token or user name and password) to boot up the system initially. A single shared account makes it difficult to revoke individual users when necessary, and in some cases violates regulatory mandates (where regulations require that each user have an individual account and credentials).

Simplified compliance: The search for an effective data at rest protection solution is frequently prompted by regulatory requirements. For example, PCI audits can result in a need for organizations to go back and encrypt certain data residing on their systems or in their network in order to meet the spirit of the regulations. The list of legislation relevant to data at rest protection includes: Payment Card Industry Data Security Standard (PCI DSS); Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (for financial services industry); Health Insurance Portability and Accountability Act (HIPAA); and the California Information Practice Act (SB1386).

- PCI: Regulations explicitly require encryption for both data at rest and data in motion. As indicated above, file encryption ensures that files are still encrypted as they travel across the network. This means that a data at rest solution can offer protection for data in motion as well, helping organizations to comply more efficiently with PCI rules.

- SOX: This legislation assigns responsibility to chief information officers for the security and accuracy of enterprise systems and the financial data reported. Data at rest encryption can help mitigate associated liabilities by making data tampering difficult, if not impossible, and making data tampering evident. The encrypted data is hard to access and even if



obtained, is impossible to decrypt. Thus, a data at rest protection solution can help with Sarbanes-Oxley compliance as well.

- HIPAA: The HIPAA security rule requires encryption of confidential data as it crosses the network as well as when it resides on systems. Data at rest encryption can help protect confidential health data in compliance with HIPAA regulations.

Ideal data at rest protection solutions also provide strong tools for compliance reporting for audit purposes, detailing statistics such as the date and time of initial encryption, and the algorithm encrypting the data.

## **SAFENET SOLUTIONS FOR PROTECTING DISK, FILE & REMOVABLE MEDIA**

### **Full disk & removable media encryption**


SafeNet ProtectDrive, a full disk and removable media encryption solution, supports a wide variety of encryption algorithms including AES-256. It provides extensive options for two-factor authentication, and also supports PKI and non-PKI tokens. SafeNet is the only disk encryption vendor that offers two-factor authentication solutions, both smartcard and USB token form factors.

Comprehensive features and versatility: ProtectDrive offers very strong key management, including separation of duties for user password recovery and disaster recovery. Removable media encryption is included as part of the encryption solution. Client machines can be configured to accept only a “company flash drive”; data stored on a “company flash drive” is not accessible on third party machines. ProtectDrive also provides port and device control, and supports current as well as legacy Windows operating systems.

Third-party validation: Extensive third-party validation for ProtectDrive comes from customers worldwide, as well as testing in approved laboratories. The U.S. Army Joint Interoperability Test Command (JITC) has recommended SafeNet to the United States Department of Defense (DoD). SafeNet is also one of the exclusive members selected to the ESI/SmartBUY program by the DoD and U.S. General Services Administration (GSA). SafeNet is currently Common Criteria EAL2 certified, and EAL4 certification is in process. In addition, the SafeNet cryptographic module is also FIPS 140-2, Level 2 validated.

Ease of use: ProtectDrive offers extensive ease-of-use capabilities. For example, it gracefully continues its initial encryption process, even after power-off/power-on or user logoff/logon events. Following such events, disk encryption continues seamlessly. In addition, Administrators find the system intuitive if they are familiar with Active Directory, thereby reducing costs and eliminating the need for extensive end user training. Furthermore, logging in and authenticating is simple, due to a single sign on option that allows for a pre-boot-to-Windows pass-through, removing the need to log in twice. Operations are transparent, without any noticeable loss of performance. ProtectDrive also supports Windows defragmentation.

*ProtectDrive is the first full disk encryption solution to deploy Active Directory (LDAP) - based centralized management, which is more robust, more familiar and less costly than proprietary management systems.*



Simplified management: ProtectDrive is also easy to manage. For example, for patch management, administrators can configure machines to enable auto rebooting through patch cycles, performing the operation over a limited period of time when computers are in a secure environment. This enables administrators to maintain the security of the mobile data fleet without incident.

ProtectDrive is the first full disk encryption solution to deploy Active Directory (LDAP) - based centralized management, which is more robust, more familiar and less costly than competing proprietary management systems. The solution also supports ADAM for Active Directory management without schema extension. ADAM is free from Microsoft.

ProtectDrive is also easy to deploy, with an MSI-based installer that can be deployed via GPO in Active Directory. In addition, it is compatible with all major software distribution tools (e.g., Tivoli, SMS, and others). Where desired, ProtectDrive can be deployed in non-Active Directory environments (e.g., Novell or other environments).

Other ease-of-use features include a reporting script for simple compliance and security auditing, helpdesk challenge/response for user password recovery, and support for a broad range of platforms, formats and disk I/O:

- Windows 2000, Windows 2003, Windows XP, Vista
- FAT16, FAT32, NTFS64, NTFS5
- SCSI, IDE, EIDE, ATA, SATA

#### **File Encryption with ProtectFile**

SafeNet ProtectFile offers a highly robust file encryption solution that can be deployed for tens of thousands of users at a time in a completely transparent manner, without any noticeable loss of performance. ProtectFile encrypts all files in designated local or remote folders, decrypts files for authorized users only, encrypts and decrypts on-the-fly without impacting performance, and allows user group access to and sharing of encrypted folders. The solution can be administered centrally or locally, with the potential to separate security management from IT administration. Features ensure real-world usability, maximum protection and reduced operating costs for data protection.

#### **About SafeNet, Inc.**

SafeNet is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect data, communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips. UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco Systems, Microsoft, Samsung, Texas Instruments, the U.S. Departments of Defense, State, and Homeland Security, the U.S. Internal Revenue Service and scores of other customers entrust their security needs to SafeNet.

For more information about SafeNet's solutions for data at rest encryption, please visit: <http://www.safenet-inc.com/DARP>