

WHITE PAPER



Addressing Issues of Data at Rest Privacy and Compliance with Strong Encryption and Authentication

How SafeNet's Data-at-Rest Protection Provides a Multi-Layered Solution

Contents

Introduction	2
Assessing Threats to Data	3
Data Privacy Regulations	4
Developing a Security Framework	5
Taking a Layered Approach	6
SafeNet's Solution for Protecting Data at Rest	8
SafeNet ProtectDrive Enterprise Version ...	8
SafeNet ProtectFile	9
SafeNet ProtectPack	11
A Multi-Layered Solution for Data at Rest Protection	12
SafeNet Overview	13

Introduction

Providing a high level of protection for sensitive information is one of the most significant challenges faced by today's enterprise network and security engineering groups. The traditional perimeter network security methods—passwords, firewalls, antivirus, etc.—provide important protection, but cannot combat all of the threats present in today's enterprise network environments. Relying on perimeter security as the sole defense mechanism, in an age when intellectual property, including trade secrets, source code, financial information, internal communications, contracts, and customer and employee information, is at the core of an organizations' assets, is simply not sufficient. An organizations' most privileged data must be 100% secure at all times.

Adding to the complexity of a secure environment is the increasing reality of a mobile workforce. Not only does sensitive data reside on various servers and workstations throughout an enterprise, but it has become pervasively transportable through the use of laptops and removable media devices, such as flash drives, memory cards, floppy disks, CDs, and external hard drives. Protecting sensitive and critical data, no matter where it resides, and ensuring that only the appropriate persons have access to that data, should be a core requirement of every company's security strategy.

Security breaches can have a far-reaching impact to not only a company's finances, but to their reputation as well. For government agencies, it may even be a matter of national security, with lives on the line. There is an expectation from customers, employees, and partners—anyone that entrusts a company with their sensitive information—that this information will be protected. Organizations must consider all of the potential damage that can be done to their business if sensitive data is lost or stolen—lawsuits, negative publicity, loss of sales and customer confidence, and permanently tarnished reputations.

It is a proven fact that only encryption can protect data no matter where it is stored. Encrypting data at rest is vital so that only authenticated and authorized individuals can view and manipulate that data. If a person or process fails to prove identity or is not authorized, access to the data is denied. The data remains confidential and the integrity of that data is achieved. And, because of its performance, ease of implementation and management, depth of security, and cost-effectiveness, encryption is an optimal solution for securing an organization's data at rest, and for addressing government and industry requirements for compliance and confidentiality.

With a strong encryption and authentication strategy at the foundation of an organization's security plan, they can rest assured that their information assets are safe, that its security practices are compliant, and that the company's reputation and brand equity will be protected.

Assessing Threats to Data

With the rising incidence of threats to sensitive data, and increasing requirements to protect that data, organizations must focus squarely on their security infrastructure. Unfortunately, it is not only external threats that must be prepared for, but internal threats as well. In fact, the incidences of data that are lost due to employee neglect or misfortune are steadily increasing. According to reports from companies made to the non-profit Privacy Rights Clearinghouse regarding data breaches and thefts, the greatest risk of exposure comes from employees or consultants who do not properly secure the data they are entrusted with.




In the last year alone, there have been scores of reports of lost or stolen laptops that contained sensitive data. This, combined with inadequate security policies and lack of oversight, place companies in a very precarious situation. Below are just a few examples of data breaches that have occurred since 2005:

- **Department of Veterans Affairs**—In May 2006, the VA learned that an employee took home electronic data that was stored on a laptop computer and external hard drive. He was not authorized to take this data home and was in violation of VA policies. The employee's home was burglarized and the computer equipment, along with various other items, was stolen. The data stored on this computer included identifying information for over 28.7 million veterans. The laptop has since been recovered and it appears that the data was not compromised.
- **Nebraska Treasurer's Office**— In June 2006, a hacker broke into a child-support computer system and may have obtained names, Social Security numbers, and other information, such as tax identification numbers, for 9,000 businesses, putting the private information of over 300,000 people at risk.
- **AIG New York**—A computer server was stolen in March 2006, containing the personal information of 930,000 customers, including names, Social Security numbers, and tens of thousands of medical records.
- **Hotels.com**—In May 2006, a laptop was stolen that contained the personal and credit card information of 243,000 customers.
- **CS Stars Insurance**—In May 2006, CS Stars misplaced a personal computer containing workers' compensation fund claim records of more than a half million New Yorkers.
- **Boeing**—In November 2005, a laptop containing the Human Resources data of 161,000 employees, including Social Security numbers and bank account information, was stolen.
- **Verizon**—In March 2006, two laptops containing the personal data of an undisclosed number of workers were stolen in a random theft and have not been recovered.

There are Web sites dedicated solely to reporting data breaches that happen around the globe, which, in itself, should provide a clear indication of how rampant the problem of data vulnerability has become. It should also provide a clear sign of how important it is to secure data at rest, no matter where that “resting place” might be. It is apparent that the most common form of theft or loss has grown to involve laptop computers and removable media. However, while outside intrusions from data thieves have been declining, they still remain a viable threat and should be accounted for when developing a security strategy.

Data Privacy Regulations

The challenge in data privacy is to protect data while, at the same time, allowing it to be shared. As Chief Compliance Officers well know, organizations should make certain that data security is the foundation of their networking policies and procedures. Today, enterprises are mandated to comply with a variety of regional, national, and/or international regulations. SafeNet makes the demand of meeting these regulations easier because when data is encrypted, compliance is often met for multiple regulations simultaneously, resulting in reduced compliance costs.

Several Examples of Current Compliance Regulations	
Regional 	<ul style="list-style-type: none"> California Database Security Breach Act (SB 1386)
National 	<ul style="list-style-type: none"> Federal Information Security Management Act (FISMA) Gramm-Leach-Bliley Act (GLBA) Health Insurance Portability and Accountability Act (HIPAA) Sarbanes-Oxley (SOX)
Global 	<ul style="list-style-type: none"> EU Data Protection Directive SOX Japan

Companies are compelled to prove their compliance with data security regulations and will be held liable for their failure to do so. The resulting penalties can include fines, heightened scrutiny, exclusion from programs, credit downgrading, legal prosecution, and, possibly, imprisonment. As an example, under the proposed Personal Data Privacy and Security Act of 2005 (U.S. Senate, Specter/Leahy), businesses that fail to implement adequate data protection practices could be fined up to \$500,000 per violation.

Encryption offers the best possible protection for data at rest, or in motion, ensuring that the confidentiality and integrity of that data is achieved, and allowing organizations to meet government regulations for protecting the privacy and security of shared information. Even if, through malice or accident, the data network is compromised, user/customer privacy and company reputation will remain intact.

Developing a Security Framework

How do organizations develop a plan to address the vast array of individual requirements, along with the persistent threats to data privacy? The answer is not by focusing on a single requirement or threat, but, instead, focusing on the single commonality shared among all—the protection of data.

Let's take a look at one example of a security framework that takes this type of approach. The **ISO/IEC 17799** is a standard for information security published by the International Organization for Standardization and the International Electrotechnical Commission, and is based on the British Standard BS 7799. The ISO/IEC 17799 standard provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing, or maintaining information security management systems. Information security is defined within the standard as the following:

- **Confidentiality**—Ensuring that information is accessible only to those authorized to have access.
- **Integrity**—Safeguarding the accuracy and completeness of information and processing methods.
- **Availability**—Ensuring that authorized users have access to information and associated assets when required.

The current version of the ISO/IEC 17799 standard contains twelve main sections:

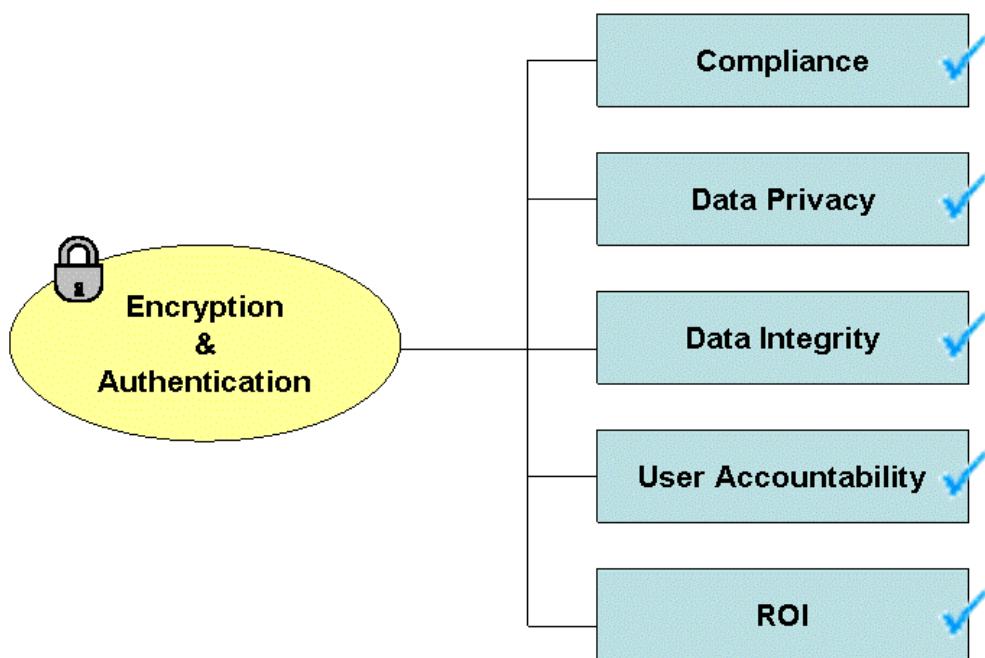
- 1 - Risk assessment and treatment
- 2 - Security policy
- 3 - Organization of information security
- 4 - Asset management
- 5 - Human resources security
- 6 - Physical and environmental security
- 7 - Communications and operations management
- 8 - Access control
- 9 - Information systems acquisition, development, and maintenance
- 10 - Information security incident management
- 11 - Business continuity management
- 12 - Compliance

In a nutshell, what is defined in a company's ISO/IEC 17799 is its "security profile"—the level of risk to take and the level of security to achieve. This would also be the profile that any partners doing business with the company must match as well. For example, in the U.K., companies that wish to do business with the government must have an ISO/IEC 17799 in place. This rule is swiftly being adopted by all large companies wishing to do business with one another in Europe.

As a result of the risk assessment phase of the security framework, a company will have a complete list of items to put into place, such as disk encryption, firewalls, backup storage, and processes for destroying information. The structure of the ISO/IEC 17799 standard allows a company to take a complete and broad approach to securing the enterprise as a whole.

Taking a Layered Approach

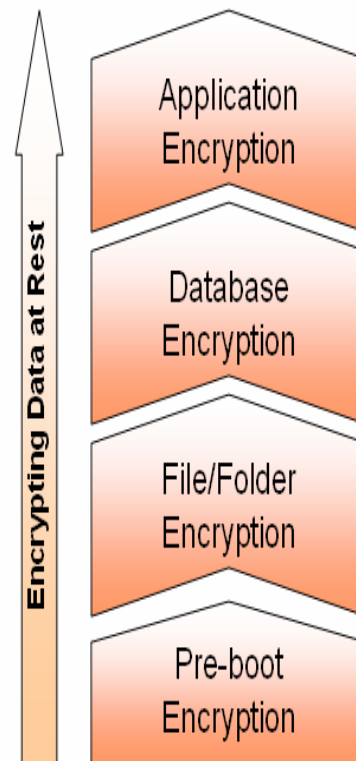
The use of encryption as the basis of any security framework provides a simple solution to many security challenges, allowing an enterprise to create a plan that provides complete data protection with a one-to-many effect.



To achieve this protection, SafeNet advocates a "layered" approach that will ensure data remains secure in any circumstance. On its own, each layer of encryption is effective, but cannot cover every eventuality. However, by encrypting data at all layers, an organization maximizes the effectiveness of its security, no matter whose hands a lost or stolen laptop, for example, ends up in. Through implementation of SafeNet's Data-at-Rest Solution products, and those of our security partners, protection at all layers can be achieved.

The SafeNet solution consists of four separate layers of protection that work together to provide a complete strategy—the more layers of security that are implemented, the stronger the protection. As with other seasoned forms of information security, such as software protection and identity management, the level of security has a direct and positive correlation to the granularity of the implementation.

- **Application level encryption** is the ability to encrypt data according to the various fields contained in the data. Mapping the encrypted fields to user privileges is done by an automated tool.
- **Database level encryption** is the ability to selectively encrypt information based on user access rights, even though the data is stored in multiple databases on multiple platforms. For example, an organization may wish to control access privileges to a Human Resources database that is distributed throughout regional centers.
- **File/folder level workgroup encryption** is the ability for end users to manage the access permissions and encryption of individual files or folders at a workgroup/user level. **File/folder level enterprise encryption** is the ability to manage server and local user files/folders from a central console based on a set of corporate policies.
- **Pre-boot and Server level encryption** provides the ability to encrypt data and require all users to produce proper authentication in order to boot up and gain authorization to access the data. This is also referred to as “whole disk encryption” and is “all or nothing”—no selectivity or hierarchical privileges accompany this level of encryption.



SafeNet's Solution for Protecting Data at Rest

As outlined in the previous section, SafeNet's solution for protecting data at rest promotes four layers of encryption for the ultimate defense against the unauthorized disclosure of confidential electronic information. The solution consists of the following:

- protecting user and server hard drives
- protecting files and folders
- protecting databases
- protecting application data

Fortified with multi-factor user authentication, SafeNet's Data-at-Rest Protection Solutions deliver the highest level of security for sensitive data on laptops/desktops, servers, and removable media devices.

It is a known fact that mobile devices containing confidential data can easily be lost or stolen, while data transmitted through a corporate network, or via the Internet, can be intercepted. This imposes considerable, and multiple, risks to organization's sensitive data. A hacker, or malicious employee/ex-employee, who might be savvy enough to penetrate through all of the perimeter security measures in force in a competent network, must still break through the most resilient of defenses—data encryption.

SafeNet ProtectDrive, ProtectFile, and ProtectPack software solutions work together to protect the storage and transmission of sensitive data on laptops, desktops, servers, and mobile devices.

SafeNet ProtectDrive Enterprise Version

Deployed worldwide by governments, corporations, and institutions to protect against security threats, SafeNet's ProtectDrive software provides the ultimate level of security by encrypting and decrypting all data 'on the fly' using strong, industry-proven certified encryption algorithms to protect confidential information residing on the hard disk against unauthorized disclosure. As an added security advantage, users are only able to access operating systems and data after successful two-factor authentication with a token or smart card. Encryption and decryption is performed transparently without additional interaction with the authenticated user, resulting in no impact on day-to-day activities.

High-Strength Encryption and Authentication

SafeNet ProtectDrive Enterprise Version encrypts the entire hard drive of laptops, workstations, servers, and removable media to protect against disclosure of information in the case of theft or accidental loss of the hardware device. Pre-boot authentication prevents unauthorized users from circumventing the operating system to access sensitive information. ProtectDrive delivers the highest level of usability to minimize application training requirements, enabling rapid user adoption across the organization and facilitating streamlined deployment.

With runtime usage of SafeNet's FIPS 140-2 Level 2-certified cryptographic library, ProtectDrive Enterprise Version meets strict government standards and ensures that confidential information is not only protected throughout operational use in the organization, it is also often implemented to make certain such data cannot be accessed when the device is passed on to the next owner or discarded.

ProtectDrive's ability to encrypt the hard disk eliminates the need for data erasure or hard disk destruction in the case of the sale, disposal, or return of leased devices.

This protection is extended to removable media devices, the use of which is on the rise within organizations. ProtectDrive Enterprise Version provides protection for removable media and introduces the "secure company medium." Once a medium is used by anyone in the company to store information, it automatically becomes a secure company medium. Only users within the company who know the password can access the medium. Employees who are explicitly granted the rights can use it outside the company's perimeter. Combined with port management and device control, which permits the configuration of allowable device types, removable media are brought under control—the result is secure media with minimal IT management and maximum user transparency.

Ease of Administration and Management

ProtectDrive delivers the ultimate ease of administration in networked environments of all sizes. No training is required for general users to derive the security benefits delivered by ProtectDrive, and only basic administrator training and knowledge is required for deployment and on-going management. ProtectDrive provides the choice of local management per workstation or full central management through Microsoft's Active Directory, ensuring that administrators work within a familiar management environment. Central management through Active Directory allows organizations to use their existing software, hardware, processes, and knowledge to centrally manage the disk encryption functionality.

Simple and automated network roll-out support through the MSI installation package, incorporating pre-definable security policies, allows quick and low-cost deployments, even in very large environments.

ProtectDrive delivers the highest level of usability available, which keeps application training requirements to a minimum, enables rapid user adoption across an organization, facilitates streamlined deployment, and keeps expenses down.

SafeNet™ ProtectFile

Adding a level of granularity to Data-at-Rest Protection, SafeNet ProtectFile file and folder encryption enables organizations to easily encrypt **individual files and folders** stored within servers, workstations, laptops, and portable media that contain confidential information. Cryptographically-enforced access rights enable only those identities with pre-allocated permission to have the ability to read, write, and modify encrypted files and folders.

Internally, data security risks have escalated in recent years due to the practice of storing data on network attached devices (file servers, workstations, and laptops) and the growing use of high capacity portable media (flash drives, memory cards, and CDs). Similarly, the level of external threats has also increased as the result of outsourced data storage and system administration. ProtectFile provides the ability to easily control individual and group permission-based access to encrypted data that is stored on various devices throughout an organization. ProtectFile encrypts and decrypts data at the client ensuring protection of confidential files in transit through the LAN or WAN, minimizing opportunities for data thieves who monitor network traffic.

For basic use of ProtectFile, no general user training or change of application operating behavior is required. All documents in a secured folder are encrypted and decrypted automatically and transparently by ProtectFile when users open and save files from within applications, or open, copy, paste, or move them in the File Explorer. A benefit unique to ProtectFile is the ability for user group managers (termed ProtectFile Administrators) to control the access rights within their user group to encrypted files/folders relevant to their area of responsibility. This separates the management of the system from its security, reducing the burden on, and liability of, network administrators.

ProtectFile can be implemented in two modes to meet integration requirements into an existing PKI infrastructure, or for de-centralized access management:

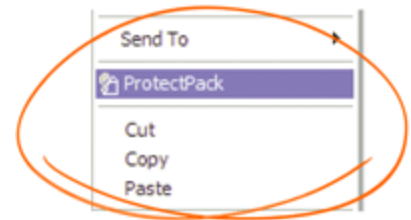
- **ProtectFile Premium Mode** works with X.509 v3 certificates using an X500 Directory and an existing Public Key Infrastructure (PKI) environment to manage users and certificates.
- **ProtectFile Business Mode** is designed for use in non-PKI environments, and allows the use of a built-in Central Management Console for user profile administration, and the creation of user groups and management of individual users, as well as the recovery of keys, and encrypted files and folders.

The silent mass-deployment function, along with pre-definable security policies, enables simple and automated rollout support, allowing both rapid and low-cost deployment in very large and small environments.

SafeNet™ ProtectPack

How can you effectively ensure a file (or group of files) remains totally confidential when sporadically transferred to another individual via a portable USB drive or floppy disk, burned to a CD or DVD, sent via email, FTP, or instant messaging, or using any other of today's or tomorrow's file mobility technology? SafeNet ProtectPack delivers the solution through secure, encrypted transfer and storage of confidential data files on unprotected mediums that are difficult to defend by conventional perimeter security mechanisms.

ProtectPack is seamlessly embedded within the Windows environment, allowing users with existing Windows knowledge to easily 'pack' and 'unpack' files. Converting to an encrypted .pac file is as simple as right-clicking on the file/folder. An authorized recipient does not need to have ProtectPack installed on their device to unpack a file. The self-extraction option attaches a compressed launch program, requiring the recipient to only enter the pass phrase to unpack the file to an unencrypted format.



An additional benefit delivered by ProtectPack includes increased data transfer and storage efficiency by optionally compressing the data before encryption. This ensures the smallest possible file size, reduces congestion and bandwidth costs within network channels, and allows increased data storage on portable media.

ProtectPack is quick to install and deploy in enterprise environments of all sizes. Administrators can rapidly and conveniently rollout the application across a Local Area Network (LAN) in the same manner as other standard Windows utilities, ensuring efficiency and minimal disruption to networked users. Also of benefit is the provision for silent installation. Administrators have the option to batch file the installation across multiple machines on a network without user interaction, ultimately resulting in both speedy and convenient deployments in environments with large user bases.

A Multi-Layered Solution for Data-at-Rest Protection

Reaching the appropriate balance between enabling communication and providing adequate protection of sensitive information is one of the most significant challenges faced by today's enterprise network and security engineering groups. With mounting regulatory considerations and an overall focus on securing data, it is more important than ever for organizations to design and implement a comprehensive plan of protection to provide not only the enterprise, but their employees, associates, and customers with the assurance that their data is secure.

The truth is that anyone with malicious intentions can gain access to data that is not properly protected. The challenge is to maintain the performance and simplicity of the network while assuring the security and privacy of user data. The answer lies with encryption, which provides organizations with the assurance that all data is protected from compromise through the strongest commercially available algorithms.

A design imperative for every SafeNet product is customer return-on-investment. Implementing a security solution must not only solve critical data protection and compliance issues, but must also be cost-effective to integrate and maintain. Organizations often see the word "security" and think "expensive." But this does not have to be the case. With data encryption, compliance is often met for multiple regulations simultaneously, reducing compliance costs. In addition, the 'Protect' family of data encryption products is essentially "set and forget." There are no significant training or administration costs associated with implementing this security solution.

SafeNet engineers security tools to be easily administered and transparent to the end user, based on open or common standards whenever possible. Thus, SafeNet security solutions are designed, from the start, to facilitate—not complicate—business processes.

Each of the SafeNet data at rest encryption products—ProtectDrive, ProtectFile, and ProtectPack—in themselves are a robust solution for the protection of electronic information that must remain confidential. When used in combination, this range of data encryption products can provide a heightened level of security. The 'Protect' family of data encryption products is designed specifically for medium to large organizations to uniquely address the industry needs of security, usability, and manageability, as well as addressing issues of regional, national, and global compliance.

With SafeNet's history as a worldwide leader in information security, companies can rest assured that they are investing not only in the highest standard of encryption technologies, but also in a vendor that will be there in the long term to support their security needs as they grow and evolve. SafeNet is one of the world's largest and most respected security organizations, and the one of the few single-source vendors to provide comprehensive and trusted information security product lines.

SafeNet Overview

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 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 and Homeland Security, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com.

Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410.931.7500 or 800.533.3958 **Email:** info@safenet-inc.com

www.safenet-inc.com

©2006 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet.

All other product names are trademarks of their respective owners.

