

## Key Features

### 100% hard drive encryption of:

- Local and remote servers, network drives, workstations, laptops
- User data, system files, hidden files, page files, temporary files
- Registry settings, hibernation files

**Strong encryption algorithm and key strength with secure key management**

**Secure two-factor authentication with optional password fallback**

**Single Sign-On to pre-boot authentication, Windows login, and other startup applications**

**Master boot record virus protection**

**Choice of centralized (server-based) or de-centralized (client-based) system and user policy management**

**Multi-boot support for up to four bootable, secured partitions, with non-Windows partitions allowed**

**Maximum transparency requiring no user interaction**

**Interoperability with existing applications**

**Easy deployment for large user bases**

**Efficient and secure data recovery**

**Remote password recovery using challenge/response mechanism**

**Secure logging of pre-boot events, such as login attempts and password changes**

**Hibernation support**

**Minimal performance loss**

**Supports rules and regulations for privacy and compliance**

## SafeNet

# ProtectDrive

## Hard Disk Encryption

*Full hard drive encryption for laptops, workstations, and servers to ensure the ultimate protection against unauthorized disclosure of data and sensitive information.*

### The Vulnerability of Data at Rest: How SafeNet Sees the Problem

Today, common threats include the misplacement of mobile devices, theft of PCs, laptops, and servers, as well as data theft when systems are discarded. The risk and severity of data theft is increasing due to four predominant factors:

- The increasing value of data stored on computers
- The increased use of laptops and other mobile devices outside the secure network perimeter
- The massive increase in the amount of data being stored
- The progressive efforts and expertise of data hackers and data thieves

These factors, and the growing number of publicized data breaches, are driving more and more rules and regulations concerning data protection and privacy.

### Transparency and Ease-of-Use

Why do we stress ease-of-use before discussing encryption strength? After all, we're perhaps best known for things like securing all voice communications on Air Force One and protecting over one trillion dollars a day in intra-bank fund transfers.

But when an IT staff cannot efficiently deploy security solutions, or end users resist adopting security measures, security suffers as surely as if one's encryption is weak.

SafeNet ProtectDrive disk encryption delivers the highest level of usability to minimize application training requirements. This enables rapid user adoption across the organization, facilitating streamlined deployment.



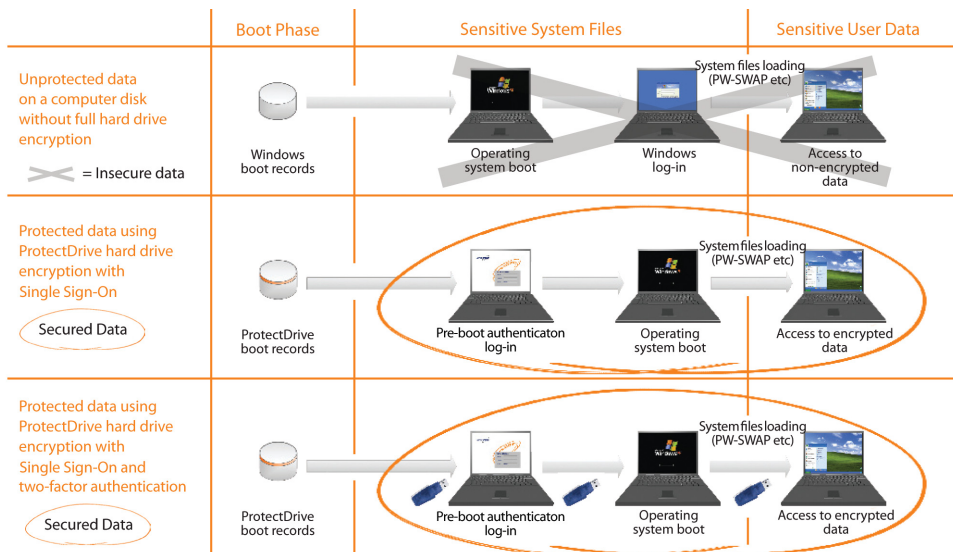
### High-Strength Encryption and Authentication

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.

### Easy Deployment and Management

ProtectDrive delivers the ultimate ease of administration in networked environments of all sizes. The integration of administration management functionality into existing management systems (such as Microsoft Active Directory) ensures that administrators work within a familiar management environment.



Demonstration of how ProtectDrive hard disk encryption secures system authentication, loading of system files, and sensitive user data in comparison to an unsecured computer.

The ability to choose between centralized (server-based) or de-centralized (client-based) system and user policy management ensures your IT management practices are not dictated by the security product architecture. This provides full flexibility to fit into your organization's existing IT security policies.

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

### Typical Applications

ProtectDrive hard disk encryption is deployed globally by a wide variety of organizations with thousands of users. Typical applications include:

- Encrypting entire hard disks of laptops, PCs, and servers against the risk of device and hard drive theft.

- Data-at-Rest Protection can be assured with ProtectDrive, implemented as a technical measure assisting to meet the increased regulation by governments around the world for strict privacy of personal information held by organizations. The Gramm-Leach-Bliley act in the U.S. for the finance sector, the SB 1386 California senate bill, HIPAA, the amended Australian Federal Privacy Act 1998, and the European Data Protection Act are a few examples of the pressures for organizations to comply with data privacy regulations.
- ProtectDrive 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 eradicates the need for data erasure or hard disk destruction in the case of the sale, disposal, or return of leased devices.

## NORDIC DISTRIBUTOR

### PERICO AS

Lilleakerveien 4, Inngang 1A  
0283 OSLO  
NORWAY

Email: [info@perico.no](mailto:info@perico.no)  
Tel: +47 22 06 40 50  
[www.pericosecurity.com](http://www.pericosecurity.com)

## Technical Specifications

### Encryption Algorithms

- 3DES, IDEA, AES-128, AES-192, AES-256

### Security Certifications

- Common Criteria EAL2 and ITSEC E1
- Common Criteria EAL4 compliance in evaluation

### Supported Platforms

- Microsoft Windows 2000, XP

### Minimum System Requirements

- 10Mb of free disk space

### Software Management Tools

- RIS, SMS, Tivoli, TNG, Active Directory, and others

