

Data Privacy



IAM for
business and people

EVIDIAN
A Groupe Bull Company

The shortest path to Data Privacy

As workforces get increasingly mobile and work teams cut across continents, there is a growing risk of theft or loss of sensitive data. Evidian Data Privacy helps enterprises to secure their information while enabling their employees and partners to work without constraints.

The Evidian Data Privacy solution comprises the **Evidian Laptop Protection** and **Evidian File Encryption** modules. These modules can be purchased independently or as a supplement to other Evidian modules.

Evidian Laptop Protection

Evidian Laptop Protection secures both fixed and mobile workstations.

Control unauthorized access to your workstations

To access their data, users must first unlock the workstation with a key stored on a removable device, then use the standard Windows login. When they leave, the workstation can be locked by removing the device. Once the workstation is locked, no operation can be performed on it.

Prevent theft or loss of sensitive data

Workstations can be registered with a specific LAN. If a workstation is taken away from this LAN, users will not be able to log on. Users will not be able to copy data to unregistered media either.

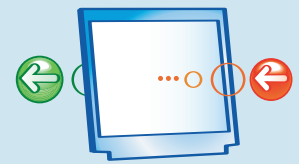
Encrypt only sensitive files or folders (not the entire drive)

You can encrypt data on the workstation or on a removable device.

Evidian Laptop Protection enables you to encrypt just the sensitive data.

Distribute a free, self-decryption runtime so encrypted files can be read easily

Distributing a free, self-decryption runtime allows encrypted files to be transferred to other employees. Thus, other employees can simply read the encrypted files.



ACCESS MANAGEMENT

3 reasons to adopt Evidian Data Privacy

1 Safer encryption process

Unlike most rival solutions, *Evidian Data Privacy* implements its security mechanisms in the file system, not in the BIOS. As a result, the recovery functions are more user-friendly, since you do not need to encrypt the entire hard disk in order to secure the most sensitive data. Moreover, in case of operating system crash, most files can be recovered.

2 Easier information exchange

With most encryption solutions, external correspondents need to own the full product to read encrypted files. *Evidian Data Privacy* includes a free decryption runtime, which simplifies deployment both inside and outside the enterprise.

3 Focus on performance

Evidian Data Privacy allows you to focus on your documents intelligently and does not encrypt program and system files, thereby improving performance.

Evidian File Encryption

Evidian File Encryption secures the sensitive information exchanged as part of collaborative work.

Evidian File Encryption allows workers to encrypt then share or transfer sensitive data between members of a project, workgroup or business process

Make sensitive data easy to encrypt and decrypt

All encryption and decryption operations are performed using right-click menus.

After you have selected one or more files or folders, the right-click menu lists encryption or decryption operations.



Automatic encryption

Evidian File Encryption enables end-users to define auto-encryption folders. A dedicated encryption key is associated with each auto-encryption folder. When one or more files are placed in an auto-encryption folder, these files are automatically encrypted.

Multiple auto-encryption folders can be defined. Thus, if an employee wants to transfer documents to several work teams, he or she can associate a dedicated key with each work team.

Prevent theft of data using removable storage media

When files are dragged or copied to a removable storage device, each file is automatically encrypted.

Share keys with internal collaborators

When the solution is deployed in an organization, once an employee has encrypted a sensitive file, he or she can send this file to another employee inside the organization (e.g. by e-mail, Skype, or Microsoft Live Messenger).

To decrypt the file, the receiving employee must share a secret key with the sender.

Self-decryption files for external partners

When employees want to send encrypted files to work teams outside their company, they just need to send a self-decryption file. This file is protected by a password.

The external partner only needs to obtain the password from the employee, double-click on the self-decryption file, and enter the security password.

To increase security, the employee can configure automatic deletion if a predefined number of wrong passwords are entered by the external partner.

Distribute a free, self-decryption runtime to make encrypted files easy to read

Distributing a free runtime makes it possible to transfer encrypted files to co-workers. Thus, other workers can easily read the encrypted files thanks to the free runtime.

Role-based administration for managing keys

Evidian File Encryption offers administration functions for managing keys: creating, distributing and recovering keys.

Reinforce security by limiting the validity of keys

Administrators may require the keys to be renewed by defining a validity period for them (e.g. the key for an organization is effective until 10/10/2008). At the end of the validity period, decryption becomes impossible.

When users leave the organization or company, administrators can also renew these users' keys.

Supported environments

Evidian File Encryption and *Evidian Laptop Protection* solutions are available on Windows 2000, XP, and will soon be available on Windows Vista.

The administration of *Evidian Laptop Protection* can be deployed in centralized mode on Windows XP or on Windows 2000 Server. This server is not dedicated to *Evidian Laptop Protection* and can be shared with any other applications.

For further information, visit our website: www.evidian.com or contact us: info@evidian.com

Evidian Data Privacy is a registered trademark of Evidian. All the cited products and brand names are trademarks of their respective owners. Evidian reserves the right to modify the characteristics of its products without prior notice