



## InfoWatch CryptoStorage Enterprise

Protect Enterprise Data against Unauthorized Disclosure and Loss while Maintaining Flexibility and Usability

### The Problem

Security breaches caused by unauthorized access to sensitive corporate information, careless or malicious employee actions with corporate data can have a crippling effect on any organization's business operation.

Confidential information has the greatest value to cyber criminals and they apply highly sophisticated methods, ranging from external hacking attacks to internal espionage and information theft, to get access to this data.

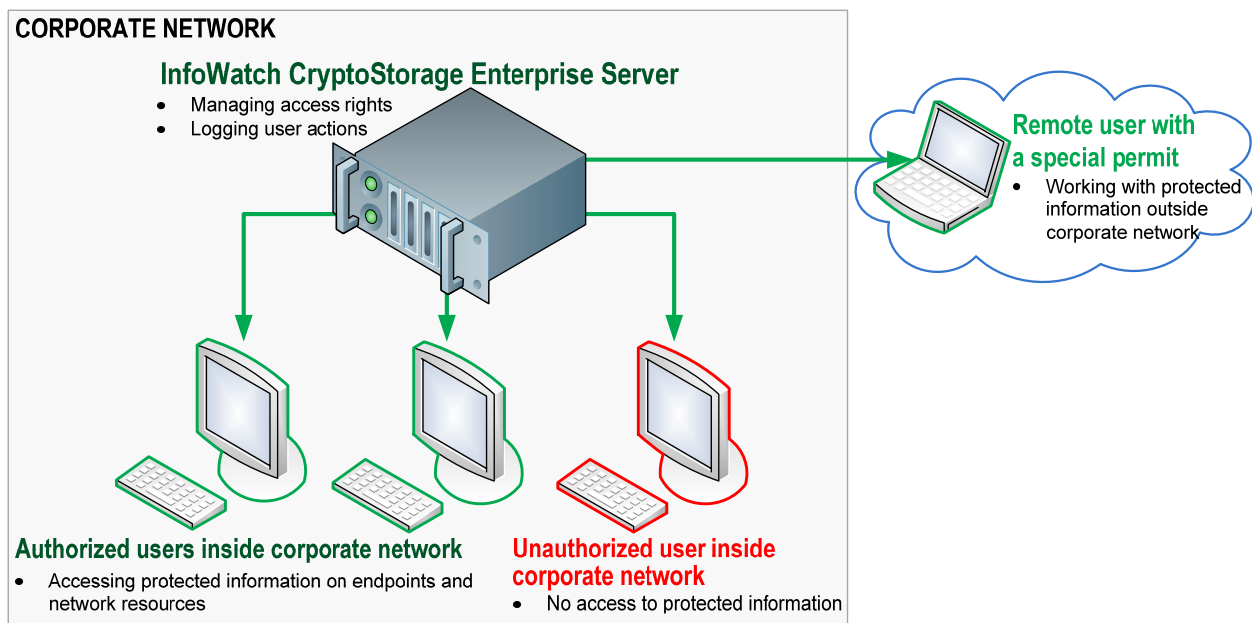
Another issue is the workforce increasingly going mobile. Today corporate confidential data, such as signed contracts or software code, market research or product launch plans, patients' healthcare records or customer information and lots of other information types, resides mostly on an employee laptop rather than in secure corporate IT environment. In this situation, loss of a device or access of unauthorized people to the information stored on it becomes much more an issue than ever before. Traditional password protection of a laptop by integrated OS tools proves insufficient, as regardless of the OS-password usage all the data from this laptop can be accessed, copied, read.

- **30%** of all data leaks happen because of laptop or mass-storage device loss or theft<sup>1</sup>
- The average value of a lost laptop is **\$49,246**. 80% of this cost arise from the **data breach** associated with such loss<sup>2</sup>
- **Intellectual property loss** accounts for the **59%** of the remaining cost<sup>3</sup>

### The Solution: InfoWatch CryptoStorage Enterprise

InfoWatch CryptoStorage Enterprise protects confidential corporate data stored on corporate servers, employee laptops, mass-storage devices, in virtual environments or cloud architectures against unauthorized access and disclosure. This client-server software product features sensitive data encryption (for laptops, desktops, USB drives, optical media, local and network folders), centralized management of information access rights and reporting.

To enable employee access to the information either a password or two-factor authentication can be used. Both approaches prove efficient in protecting information against unauthorized access. Integrated resilience tools allow restoring access to the information in case of system errors during encryption.



<sup>1</sup> InfoWatch Global Data Leakage Report

<sup>2</sup> Ponemon Institute. *The Cost of a Lost Laptop*

<sup>3</sup> Ponemon Institute. *The Cost of a Lost Laptop*



To contribute to business continuity and to securely recover access to the protected information in case the employee leaves the company, forgets the password or loses secret key, InfoWatch CryptoStorage Enterprise includes a recovery committee feature. This feature can be enabled by product setup. The recovery committee includes several trusted employees (InfoWatch CryptoStorage Enterprise users) whose secret keys can be used to restore access to the encrypted information. For additional data security the access can be restored only when secret keys of certain, specified by product setup number of recovery committee members (quorum) are available.

Encrypted information (copied to a USB, for example) cannot be accessed outside corporate network even by an authorized user without a special permit, issued by the InfoWatch CryptoStorage Enterprise server on a case-by-case basis. All actions with protected information are logged and stored for further analysis.

## Data-at-rest protection and cloud security

InfoWatch CryptoStorage Enterprise features protection of information on local machines, in network repositories, virtual environments and cloud architectures. Encrypted information can be read only by its owner or users whom the information owner allowed access. No matter where in the cloud the data is stored – it is accessible only to authorized users and is perfectly secure.

## Safe hardware repair and green hardware disposal

With InfoWatch CryptoStorage you can protect whole hard drives or their partitions. It is the safest way to prevent sensitive information leakage that can happen while repairing your PCs or laptops in service centers or disposing of hard drives in specialized hardware disposal agencies.

## Removable mass-storage device protection

With InfoWatch CryptoStorage Enterprise you can protect information stored on various mass-storage device types – USB drives, optical media, memory cards, etc. You can copy all the data you need to a removable mass-storage device and physically move it to another location. No data breach will happen even in case of device theft or loss.

## Secure collaboration

InfoWatch CryptoStorage Enterprise protects information both on endpoints and in server repositories, to enable smooth and secure employee collaboration. Hierarchical multi-user access to the encrypted information with centralized access rights management can be easily set up. For example, employees from Microsoft AD group “sales” will have access to customer data, while the same information will not be available to the “IT” group members. The product allows protected information access outside corporate network with special permits.

## InfoWatch CryptoStorage Enterprise Benefits

### Unprecedented data security and ease of use for corporate employees

- Centralized setup and management with high access rights granularity
- Multi-user hierarchical access to protected information
- Recovery committee feature to restore information in case of password loss
- High performance during encryption and decryption
- Single-Sign-On mechanism and transparent on-the-fly encryption / decryption not to interfere with regular employee activities
- Special permits to enable working with protected information outside corporate network
- Centralized logging of all actions with protected information for extensive customizable reporting
- Strong encryption algorithms used: AES 128/256

### Additional product features

- Prevention of unauthorized data deletion or modification – encrypted information cannot be accidentally or intentionally deleted or modified by unauthorized users
- Guaranteed deletion of information – the data deleted with InfoWatch CryptoStorage cannot be restored even with specialized recovery programs that work perfectly for information deleted with regular OS tools
- Protection against data sniffing: the protected information stored and transmitted encrypted. It is decrypted in the RAM-memory when the data is being read (the file is being opened) and is automatically encrypted on closure
- Resilience to system errors during encryption

## Your Gains

- Management and **mitigation of financial, legal, reputational and other information-related risks** associated with data loss
- **Compliance** with internal policies & standards, external rules and regulations, industry standards (for example PCI DSS, SOX, GLBA, HIPAA) and customer security requirements
- **Cost transparency and low TCO**: unlike with the competitive solutions, all product functionality is available inside a single module. No additional component licensing is required.

#### System requirements

- Client side: OS - MS Windows (XP, Vista, 7, 2003, 2008 R2). Hardware: Celeron 1GHz and higher, RAM 256Mb, 30Mb of hard drive space.
- Server side: MS Windows (XP, Vista, 7, 2003, 2008, 2008 R2). Hardware: Pentium-4 3 GHz, RAM – 1Gb, 30 Mb of hard drive space