

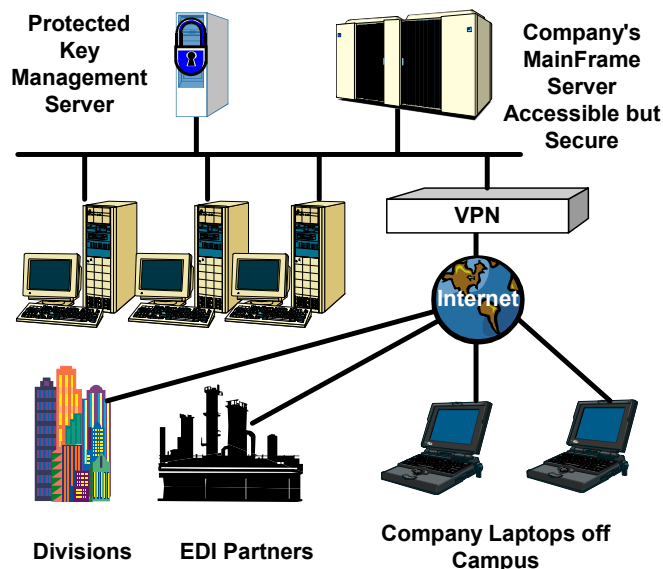


## CryptSec™—Securely Enforcing the Need to Know

VizorNet supplies enterprise and network information security systems designed to meet previously-unanswered needs of the Government and business communities for information security and need-to-know control at the highest levels, with demonstrated *5 minutes time-to-learn, protection against insider data compromise, a solution to the “lost laptop” problem, and retroactive denial of access to those leaving the enterprise, even if they take files with them.*

VizorNet solves the "lost laptop" problem, the "wandering CDROM" problem and the problem of data compromise by insiders and consultants—and enforces need-to-know.

- 591,000 laptops were lost or stolen in 2001 (recent IBM statistic).
- According to the FBI, 84% of recorded computer crimes involve the cooperation of insiders—including consultants with network administrator privileges.
- Pharmaceutical Manufacturers, have estimated that a single compromise of one key piece of intellectual property, e.g., a developmental drug, causes a loss in excess of \$100,000,000 to the enterprise.
- Compromise of critical financial or strategic information can not only damage an enterprise, but also lead to criminal sanctions.
- Yet...nearly every networked enterprise has employees and consultants with administrative access who can read, copy and modify files almost at will, often by just monitoring the network.



# The Challenge: The Weakest Links in the Chain

We demand and get instant access to information in today's digital age. This capability has fostered the often rapid sharing of data, documents, images and all other information elements in the highly open Internet, and throughout business and government "private" networks. With a single "click", information can be sent to almost anyone, across networks, operating systems, geographic boundaries, even to space. For the protection of government and business sensitive information, we rely today on document classification, closed networks, encryption, honoring the "need to know" policies, and other techniques. However, the weakest link in the chain of information control remains the human element.

## Breaking the chain

Envision how the information chain of control is most often broken: wrong or illegal cross-fertilization of data among internal employees; insider data theft and compromise; access to information by outside technicians and staff having network or computer access; staff taking laptops on travel and losing them; Electronic Data Interchange (EDI) with suppliers and clients; remote access to data files by staff; and other means.

## Protecting the chain

Automating the control of information sharing based on the "need to know" is a major CryptSec™ capability. CryptSec™ is built on the global Advanced Encryption Standard (AES), developed under the auspices of the U. S. National Computer Security Center and Department of Commerce and intended to be used by both U.S. and other international governments as well as national and international businesses. It incorporates proprietary patent pending multiple key software encryption whereby the user has only one of the multiple pairs of keys needed to unlock the data that is being protected. Critical information cannot be accessed without being on or within the key domain that contains a second key which is provided by the CryptSec™ key server—and *never appears on the network.*

## CryptSec™ deals with the human element

- **Enforces** security of vital data - no unauthorized user options
- **Prevents** unauthorized insider access to data - **even by administrators**
- **Works** with your existing network, data systems and EDI
- **Protects** data on "lost" laptops and disks, and against unauthorized E-mailing of data
- **Retroactively** denies access to an employee departing with files
- **Provides** an unchangeable evidence log of sensitive data actions

- **Solves the problem of weak, easily discovered passwords.**

## **Insider-compromise Protection**

CryptSec™: advanced enterprise security with many unique features:

- Prevents unauthorized access, even from a trusted *insider* source
- Encrypted positive ID - assigned, easy to memorize (but very secure) passphrase. No “easy” passwords allowed. Passcodes are never stored at the workstation or laptop
- Ignition-key option based on US Government technology
- Transparent to user – less than one hour or less user training
- Permanently logs of all data accesses, providing a chain of evidence
- No degradation of LAN, WAN or VPN performance
- Not compromised by backup storage
- Allows for the creation of shared groups that cross folder boundaries
- Group membership can be altered without the need to redistribute keys to existing members
- Member revocation is controlled by the group owner or Security Officer, and is retroactive
- Restricts printing of protected documents, without proper key authorization
- Solves the unauthorized data access problem due to a lost laptop
- Solves the problem of disappearing CDROMs and unauthorized emailing of vital data by insiders.



CryptSec™ manages sensitive data on a multilevel security basis, and where necessary, works within the envelope of government or business end-to-end cryptosystems, thereby providing security control not otherwise available.

## **Basic Functions**

High-quality enterprise-level network information security suite focusing on ease and transparency of use, one-hour user training, and protection of authentication and access against user mistakes; as well as prevention of (often ignored) insider data theft.

Security is achieved by the use of multiple key technology, optionally including physical VizorKeys which users can carry on their keychains without risk of compromise if lost. Functionally similar to US Government CIK (crypto ignition key) technology.

### **Threere layers of keys are used:**

- 1. A Personal key** in the form of an assigned passphrase, easy to memorize but very hard to discover: There are about 578 Trillion options. The use of a physical VizorKey increasesd the complexity to the magnitude of the number of atoms in the Universe, without memorizing anything., and can be used in conjuncion with a personal key.
- 2. A Network key** in the Keyserver, required for encryption and decryption, but *never transmitted outside the keyseerver.*
- 3. A Workstation key (optional)** which associates each user with the specific workstaions which may be used by that person or security domain. The workstation key cannot be recovered by "dumping" the workstation files.

### **Workstation Integrity**

A secure technology is used to insure that critical algorithms in the workstations have not been tampered with, nor compromised by spyware. Details are not disclosed here. The Cryptsec KeyServer is similarly protected, but in addition is accessible by only one or two designated individuals in the enterprise—not the entire administrative staff contingent.

### **Other Technical Features**

Most important is transparency of use, in which users have little or no learning nor interference with their daily routines, and the solution is transparent to applications and operating systems.

Implementation of individual features depends on client's security protocol, which specifies what attacks or losses are to be prevented.

Operates at the OS level inside the client, and Layers 3 and 4 (network and transport) on the network; hence is transparent to data structure and application. Compatible with most ethernet, internet, intranet, and VPN networks, Windows client operating systems and any data storage system. Does not alter the enterprise data storage system.

Works with EDI partners who do *not* share the enterprise's security system, but have limited read-write access.

Enforces need-to-know through directed-graph security compartmentation (X may be entitled access to B and C, while X may be entitled to C and D).

Patent-pending methodology uses the approved National Institute of Standards and Technology (NIST) and US-Government certified encryption methods, planned for FIPS certification.

Another patent-pending methodology allows each file to be authorized access by multiple approved groups of users, without the need to store separate copies of that file for each user. This simplifies workgroup collaboration (where permitted by the security rules) without violating the security rules themselves.

The enterprise system utilizes approved US Government key management technology including optionally a cryptography ignition key which the user can safely carry on a key chain (see photograph above), and was pioneered for the Government by VizorNet's chief scientist. A small CryptSec Key Server on the network is the only hardware that needs to be physically protected with rigorously limited access. Key server assigns session keys to every data transaction and logs all data accesses (in and out).

All data to and from storage (local and server) are encrypted and decrypted. Provisions are made for laptop use off-site for designated files, for limited time periods.

Multiple Keys are partially stored in authorized client machine, partially stored on the user's VizorKey, partially stored on the authorized workstations (if desired) and partially stored in the Key Server. *All keys must be correct in order for the data to be accessible.*

Optionally the user may be assigned a passphrase which unlocks read-only access to the VizorKey, or provides user authentication (depending on security protocol).

### **Authorized Use of Laptops on "Away Missions"**

When the laptop leaves the premises, all of the data on the laptop are already enciphered. The user must be connected to the network for full access, or receive a time-limited token to open certain files for, e.g., a presentation. Works with internet and intranets, VPNs. LANs. Works with the client's own firewall. Features include protection against weak passphrases by assigning passphrases that are strong yet easy to memorize, delivering them securely from the Key Server.

For some installations the keyserver may be duplexed as a nonstop subsystem.

For the occasions where a laptop is used for g.e., a presentation and online connection to the KeyServer is impossible, special short-time provisions are made for individual files (such as presentations) to be under user control.

### **For Additional Information:**

CryptSec™ is a product of VizorNet™, Inc. VizorNet specializes in advanced software encryption products for government and business, which protect sensitive data shared in collaborative operating environments. In addition, its professional services provide a total security solution ranging from information security, network security and operational security, as well as project management, quality assurance, contract implementation and business development. Additional information on CryptSec and VizorNet may be obtained at [www.vizornet.com](http://www.vizornet.com) or by calling 703-966-9536 or 866-938-7800.

**CryptSec™ — Securely Enforcing the Need to Know**