



Where do you store the “keys” to your enterprise?

Network Vault[®]

**Solution Overview:
Securing the Vital Information of the Security and System Department**

**When all the walls collapse, the Network Vault[®] is still there
to protect what you must never lose...**

Hermetically Securing the Network - Mission Impossible

The corporate network is too complex an environment to secure in its entirety. Computers and computer networks were made for functionality, openness and accessibility, not for securing sensitive objects. Many organizations have gone to great lengths to build state-of-the-art security solutions in ways that are comparable to creating a fortress.

Yet, after implementing all existing security measures, you can still never *really* know if the “crown jewels” of your enterprise are protected from loss and exposure.

The Challenge: Where do you store the “keys” to your enterprise?

Every enterprise relies on a few priceless data items that must never be lost or exposed. The danger of losing or exposing these items is vital to the enterprise’s business continuity and can even threaten its very existence. Prior to the Cyber-Ark[®] solution, the enterprise network could never be considered secure enough to safely hold the crown jewels of the security department, such as:

- *Emergency Passwords*
- *Encryption Keys*
- *Security Assessment Reports*
- *Root Certificates Keys*
- *Disaster Recovery Plans*
- *Security Policy Documents*

The potential damage to an organization in case of exposure or loss of these valuables must never be underestimated. Gaining control over the priceless information of an organization’s security department could enable control over its entire IT infrastructure and therefore over its organizational processes. Exposure of Emergency Passwords or Root Certificates Keys could enable a potential insider or intruder, to intervene or disrupt critical business processes such as financial transactions, manufacturing processes, or the provision of healthcare or infrastructure services. Consequently, in many sectors, physical forms of such valuables are protected in physical safes and by dual control procedures. Moreover, in some cases, these physical security measures are even enforced by formal regulations.

Introducing the Network Vault[®] - Protecting your vital information

Cyber-Ark[®] employs the concept of a physical vault to secure the enterprise’s most valuable information, by providing the **Network Vault[®]**, a *Safe Haven* over the network, which is isolated from harm, yet accessible. It is a long-term repository, highly secured regardless of overall network security and regardless of the physical topology of the network. It is the most effective way to *protect and control* critical information.

The Network Vault[®] enables you to be certain that even if all the walls within and surrounding the network collapse, you will *never* lose control over the most critical assets of the enterprise.

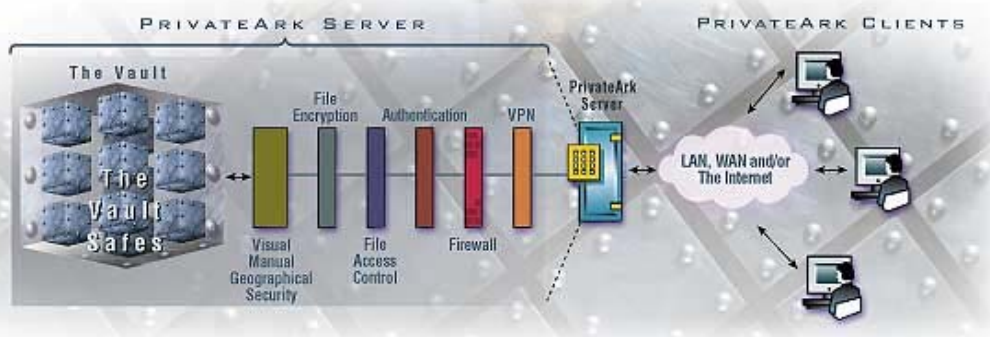
10 Security Layers provide the first End-to-end Security Solution

With the Network Vault[®], your priceless information is immune from loss, corruption, and exposure. 10 security layers - including VPN, Firewall, Data Access Control, Encryption, Authentication, Secured Backup and more - were designed and built from the ground up to create a highly secured repository that offers end-to-end protection.

The Vault provides full control over each data item, full auditing capabilities, and enables dual control over the information stored inside the Vault. The Vault was named “Best Security Product of 2001” in the Networking Industry Awards, and is considered by industry experts to be the most secure solution available today for information storage over a network environment.

Using the Vault your priceless information is protected:

- while it resides in the Vault
- during transmission over the network



Data stored in the Vault is protected from all major security risks, including Man-in-the-middle attacks, Host-based attacks, Buffer overflow attacks, the threat of viruses, vandals or Trojan Horses, Sniffing, Spoofing and more. The Vault’s architecture was designed to ensure that the data is safeguarded from known, unknown and new security holes.

The Breakthrough is in the Vaulting Technology...

The Network Vault[®] architecture is based on Cyber-Ark’s **Vaulting Technology** (US Patent No 6,356,941 B1). Cyber-Ark[®] discovered that by splitting the server interfaces from the storage engine, it can remove many of today’s technology barriers associated with network security. The Vaulting Technology creates a Single Data Access Channel, which significantly improves security and makes it possible to build 10 layers of security in a unified solution.

Visual Security™: Security you can see

For the first time, your data security is visible. A unique patented technology enables owners of information to actually see, what happens with their information at all times. It enables end-users to receive visual indications of accesses and updates to objects in the Vault. The Visual Security indications are automatically displayed as users go through their daily workflow.

Visual Security serves as both an audit and deterrent tool. By using it, you will be aware of every access or change to your vital information.

Dual Control and more: Security you can bank on

A dual confirmation may be required to open certain safes inside the Vault, similar to the requirement for two keys to open a safe deposit box in a bank. When attempting to open such a safe, a request for clearance will be sent to the safe's supervisor(s). The safe will only be opened after such access is confirmed.

Using this advanced feature, emergency passwords, for instance, cannot be retrieved and used, under any circumstances, unless security manager(s) have confirmed such access.

“The Company security system must be designed such that no single person has full knowledge of any single encryption key. This must be achieved by separation of duties and dual control.” excerpt from a Fortune 500 company's security policy.

Delay

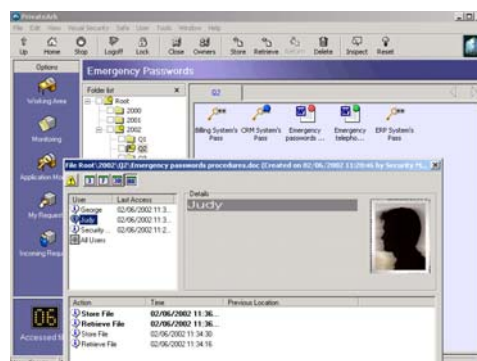
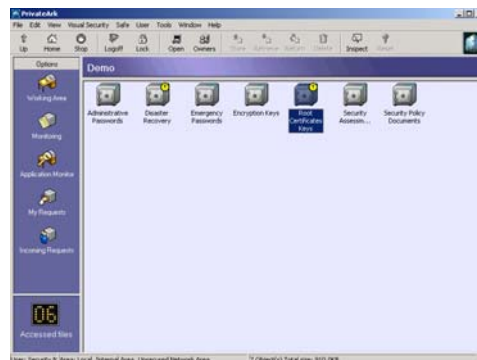
A unique mechanism enables delaying the opening of a Safe for a predefined period of time, allowing supervisor(s) to prevent unwanted access.

Time limitations

A Safe can be defined to allow access only within certain time frames, such as during working hours.

Geographical Security

The Network Vault® can limit access to users and safes to certain network locations. Thus, the security assessment reports, for example, can only be accessed from certain rooms and not from the rest of the building.



Key Benefits

- **End-to-End Security** – The Network Vault[®] provides the highest level of security available today for critical information.
- **Assuring Business Continuity** – The Network Vault[®] enables the enterprise to protect its vital information assets from loss and exposure, thus ensuring business continuity.
- **Auditing and Control** – The Network Vault[®] provides a comprehensive auditing and object-level control required for vital information assets.
- **Rapid Deployment** – The Network Vault[®] provides military-level security in a ready-to-use solution that requires little to no security expertise.

Technical Specifications

The Network Vault[®] supports major industry standards and protocols:

Encryption and Hash algorithms:

- 3DES, IDEA, Blowfish, RC2, RC4, RC5, RSA, SHA1, MD5

Authentication Methods and Devices:

- Password based - Two way Challenge-Response
- PKI
- Windows NT based Authentication
- Cyber-Key
- RSA SecurID
- Smart cards

Supported Platforms:

Server:

The Vault server should be run on a dedicated computer.

- Windows 2000 - Professional, Server, Advanced Server

Personal Client:

- Win9x with Internet Explorer 4 or higher.
- WinNT SP5 or higher with Internet Explorer 4 or higher
- Win2000 SP1 or higher
- WinXP

About Cyber-Ark® Software

Cyber-Ark Software Inc., is the leading provider of vaulting security software that leverages its unique patented Vaulting Technology to create safe havens for securing and sharing vital company information. The company's award-winning Network Vault® and Inter-Business Vault™ solutions enable a truly secure extended enterprise by providing an infrastructure that allows for completely transparent, yet totally secure, intra- and inter- business communications.

Founded by a group of leading military security experts and computer engineers, Cyber-Ark Software is privately held and backed by some of the world's most successful venture capitalists, including: Jerusalem Venture Partners, Seed Capital Partners (a SOFTBANK Affiliate), JP Morgan/Chase Partners, Vertex Management and Nomura International Plc.

Awards



Cyber-Ark's solution was awarded "Best Security Product of the Year 2001" by the renowned Networking Industry.



"Cyber-Ark offers the most elegant and efficient solution we have seen to the problem of securing confidential data in a networked environment where sharing is important but must be properly authorized and user authenticated." ★ ★ ★ ★ ★

SC Magazine, Nov 2001

Cyber-Ark® Software, Inc.
270 Bridge Street
Dedham, MA 02026

Tel: 1-888-808-9005

Tel: (781) 251-0670

Fax: (781) 251-0678

sales@cyber-ark.com

www.cyber-ark.com

© 2002 Cyber-Ark Software, Ltd. All rights reserved. US Patent No 6,356,941. Cyber-Ark®, the Cyber-Ark logo, the Cyber-Ark slogan, PrivateArk™, Network Vault®, Inter-Business Vault™, Geographical Security™ and Visual Security™ are trademarks of Cyber-Ark Software Ltd. All other product names mentioned herein are trademarks of their respective owners. Information in this document is subject to change without notice.