

Review

Under lock and key: internet networks and external threats

Private Ark uses real-world scenario of locking items in a vault which is only accessible with the right key, reports *David Ludlow*

The office today expands beyond the standard four walls. Companies have divisions spread across the world and road warrior workers tied to a laptop and company car. Despite this, modern day communication still allow for these diverse groups to collaborate on documents.

Various people in different places accessing information on the corporate network can pose a security risk. Networks were designed to make it easy to share data, not necessarily to keep it safe.

For example, it is typical for users to share documents via email, but when that information is confidential, can email really be trusted?

All it takes is for one user to leave a laptop lying around or a typographical error in an email address and confidential data will end up in the wrong hands.

To ensure that information is kept safe, think about how you can protect the internal network from the external environment

Choosing a VPN

The most obvious tool is a firewall. A policy should be implemented which states the type of traffic that can and cannot be run in and out of any corporate network.

It is then easier to apply rules to a firewall and lock



out unwanted visitors. But what about the external users who need to break through the firewall?

Install a VPN. This technology extends the corporate network across a public network – such as the internet – by using encryptions and protection. It makes remote access very cheap, as users only need a local dial-up connection to access the corporate network. As broadband technologies slowly roll out, VPNs are making more sense.

It used to be that installation of a VPN would require additional hardware, but it's common to find the service on a firewall. Don't worry about performance,

as firewalls have the hardware to cope with both tasks.

The only thing to look out for is additional charges for the VPN service. CheckPoint charges extra for a VPN licence. If you buy Nokia hardware, then you will also have to buy the VPN module. This isn't standard. For example, NetScreen includes the VPN service as part of its package, and you are not penalised for using it.

It is also necessary to secure digitally stored data for internal and external users. The typical approach is to store information on multiple servers through the network, making their security network-focused. This is the wrong approach, however.

Cyber Ark's Private Ark Network Vault

follows the real-world scenario of locking valuable items inside a vault so only those with the right key have access. It centralises storage in an encrypted database stored on a single NT server. Around this, the software also provides a host of security measures. These include a firewall, VPN, authentication, access control, encryption code isolation and virus protection. The firewall is a network device driver that acts as a packet filter. If the Private Ark server is down, the firewall does not permit any packet in or out of the machine.

Once the server has started, the firewall will only open the port that the Private Ark server is running on. This prevents any other software on the machine from being communicated with, even if a Trojan was installed.

The VPN function encrypts all data transmitted between a client and the vault and prevents data being stolen, for example, through the use of a sniffer.

Code isolated is there to protect the server. While the software will allow executable files to be stored in the vault, it will not allow any of this code to be executed. This makes sure that, beside the OS, Private Ark is the only program running.

Authentication is an important aspect of this

software. It can use either the built-in two-way protocol or a third party. Support for this is provided by PKI certificates, RSA SecureID tokens or standard NT domain authentication.

Virus protection guarantees that a vault is completely free of all infection. It does this by refusing to store any files that are executable or that contain executable code.

Before we looked at the product, we installed a fresh version of WindowsNT, making sure only the minimum number of components were installed. The server needs to be completely clean for installation to work.

The manual talked us through the cleaning steps, which included removing all network services and modifying some registry keys. Once this is done, the main installation is ready to be performed.

Security back up

This is a surprisingly quick operation, and the only user interaction is to tell the server where the vault's encryption key is stored. For additional security, the key should remain on the provided CD. This way, once the Private Ark server has started, they key can be removed and stored in a physical safe.

If the server is stolen or rebooted by a third party, Private Ark won't even start, leaving your data completely safe. Of course, as the CD can be lost or damaged,

Cyber Ark provides two CDs with the keys on, and two master keys, which can be used to recover a vault in the event of a problem. Once the server is up and running, there are two methods of accessing it: through the client or through a web browser.



The client has the advantage of integrating itself with Explorer to make it easier to deal with stored files. However, the standard interface is the same for the web version, which can be used from anywhere.

A price to pay

Logging on displays all the vaults in the system. Standard users will only be able to see the vaults that they created or have been given access to.

Opening a vault is like opening a directory. The list of stored files is displayed. When a file is opened up, the software retrieves a

file into a protected workspace on your computer.

This keeps the file protected and makes sure any changes are written back to the vault. The vault will also track changes and who made them. The owner of the vault can see exactly

Having said that, once the software is up and running, it offers the most secure method of storing files we have ever seen. With digital storage becoming more and more important, you are going to need a vault like this that won't let you down.

David_Ludlow@vnu.co.uk

what has happened to a file and, if needed, return to a previous version.

Overall, we were impressed with the software. It will offer the protection you need to secure confidential files, but you've got to be willing to pay the price. It is not a cheap piece of kit, so it isn't an option for all corporations.

We've also heard from some customers that dealing with upgrade can be painful. It can apparently introduce access problems in addition to a difficult server upgrade procedure.

Product Details

Cyber Ark - Private Ark

Price £11,495

Contact:

GSS 0870 458 1113

www.gsec.co.uk

Pros: Very Secure; provides good access mechanisms

Cons: Expensive, handling upgrades can be difficult