

The Iron Mountain Online Backup Solution for Servers

A practical guide to Iron Mountain's security and protection of your data

Iron Mountain Server Electronic Vaulting security features

WITHOUT YOUR DATA, THERE IS NO RECOVERY

In today's security conscious environment, many organisations are looking to online backup solutions as a cost effective solution for data backup, vaulting and recovery. A complete and secure online backup solution, providing organisations with the highest level of digital and physical data security, allowing them to feel fully confident that their information is reliably backed up and protected not only from authorised access, but also from natural, terrorist and environmental threats – during all phases of data transmission and storage.

COMMUNICATION PROTECTION

- All communications use outbound only connections via specific ports.
- All connections are authenticated and authorised.
- Digital certificates authenticate senders and receivers
- All communications are further authorised via central management (Agents can only talk to our authorised vaults)
- Backup data is encrypted using customer private keys to 256 AES encryption levels, the highest level available.
- Customer can be the sole owner of the data encryption password/key or escrow the key via Iron Mountain's Intellectual Property Management Division.
- Web portal communications are further encrypted using SSL

SECURITY: NO SPOOFING

Public key/private key digital certificates used for mutual authentication so that the agent software can verify that outbound connections are to an Iron Mountain vault and the vault software can verify that a connection is coming from the customer's server.

- Username and password used to access the web user interface
- A password policy can be created, allowing frequency of change and size and make up.

- Specific retention policies can be applied to backup policies allowing automated or manual destruction of digital records dependant upon the policy. Options available are 30 days, 60 days, 1 year, 3 year and 7 years. Bespoke retention options are available upon request.

SECURITY: NO EAVESDROPPING

Data Encryption Overview

- All data is encrypted with the 256 bit AES algorithm
- Data is stored encrypted on the Iron Mountain vault and on any on site storage appliances.
- Data restored on media (NAS device) is encrypted
- The customer and only the customer has the key
- Data physically resides at a highly secure, class A, data centre, not a co-location facility – Data centre uses best practices for physical security, including dual comms, power, UPS, mirroring, and CCTV security
- Password reset is available should an administrator leave. Previously backed up data (and new data) is recoverable with the new password. The old password will not work on either new or old data
- The data encryption password is associated with a server
- It's NOT the user password to access the web UI

USER INTERFACE SECURITY

- A stolen username / password does not provide access to data
- No data can be viewed via the user interface
- Data can only be restored to a server that has the data encryption password for that data
- The server where the data originated, or another server on which the data encryption password has been installed
- Installing a data encryption password cannot be done through the web user interface. It can only be done by the system administrator with console access to the server who knows the data encryption password

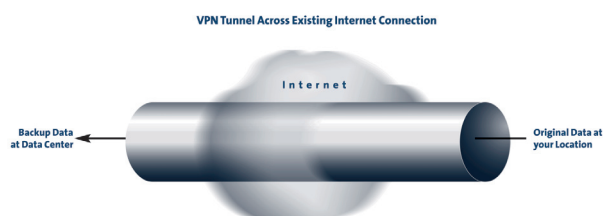
WHITE PAPER

IRON MOUNTAIN - ONLINE BACKUP SOLUTION FOR SERVERS

SECURITY: NO CORRUPTION / MODIFICATION

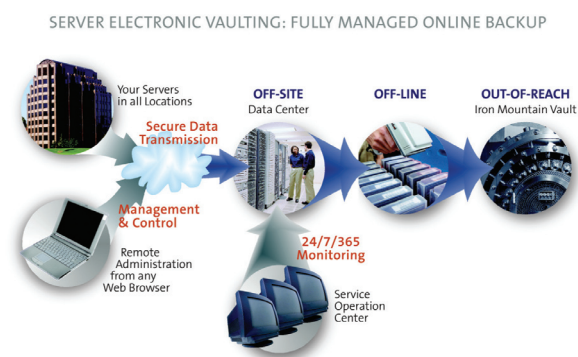
Digital signatures

- All network packets are digitally signed
- Packets that are altered in transmission, accidentally or maliciously, are rejected and resent.



THE IRON MOUNTAIN SOLUTION

Online backup, offers the most advanced digital and physical security standards for data backup, vaulting and recovery. The digital security standards employed include digital certificate authentication, digital signatures, AES encryption during transmission and in Iron Mountain's vaults, together with VPN tunnelling. All changes to business critical files such as email, databases, and file servers are continuously transmitted via the Internet and securely vaulted at an Iron Mountain vault.



HOW IS YOUR DATA BACKED UP TO OUR VAULT?

Iron Mountain's online backup product uses snapshot technology to send your data as frequently as every fifteen minutes to our secure vault automatically. You can choose a policy to send snapshots every 15 minutes 24/7 or schedule a time more suitable if required.

Our technology sends data at Delta block level. This means only the incremental changes in data are sent to our vault, rather than the whole file. Furthermore, the data is encrypted and compressed before it is sent to Iron Mountain's vault. This allows for very economical use of bandwidth.

HOW DO SNAPSHOTS WORK?

This is a file system feature that allows you to preserve a "point in time" view of a volume or partition. The backup is fully automated, no manual intervention is required. Each time a block is written, the before image is saved "off to the side". If your policy is to backup every 15 minutes a snapshot "point in time snapshot" image will be created for backup. You have the ability to recover the current data and any snapshot you have created over time. The number of snapshots held by Iron Mountain is based on your retention policy. The snapshot is created whilst allowing on going updates to take place. Any changes made during the snapshot will be stored ready for the next snapshot. This includes any open files. A filter driver (kernel level code) is used to collect information about snapshots to allow efficient backup.

SNAPSHOT FORMATION

The snapshot technology asks the Volume Shadow Copy Service to prepare for shadow copy creation. The Volume Shadow Copy Service notifies the application-specific writers to prepare their data for making a shadow copy. The writer prepares the data in whatever way is appropriate, such as completing all open transactions, rolling transaction logs and flushing caches. When the data is prepared for shadow copy creation, the writer notifies the Volume Shadow Copy Service. The Volume Shadow Copy Service initiates the "commit" shadow copy phase.

WHITE PAPER

IRON MOUNTAIN - ONLINE BACKUP SOLUTION FOR SERVERS

The Volume Shadow Copy Service temporarily freezes requestor (application) I/O write requests (I/O read requests are still possible) for the several seconds required to create the shadow copy of the volume or volumes. The application freeze is not allowed to take longer than 60 seconds. The Volume Shadow Copy Service freezes the file system, which ensures that file system metadata is written and that the data is written in a consistent order.

The Volume Shadow Copy Service creates the shadow copy (a maximum of 10 seconds). The Volume Shadow Copy Service thaws the file system. The Volume Shadow copy Service queries the writers to confirm that write I/Os were successfully held during shadow copy creation. If the writer were not successfully held (meaning that the shadow copy data is potentially inconsistent), the shadow copy is deleted and the requestor is notified.

The requestor can retry the process (go back to step 1) or notify the administrator to retry at a later time. If the copy is successful, the Volume Shadow Copy Service gives the location information for the shadow copy back to the requestor.

DATA REPLICATION ON SITE/OFF SITE OR OFF SITE ONLY

Not only does our software give a customer the ability to have an off-site copy of their data using Iron Mountain's On-line backup but also available is an onsite backup device. This hardware device, provided by Iron Mountain, takes snapshots as per the backup policy and provides an onsite LAN/WAN capability for restores. Should a hardware or software error occur on the client's production servers the data can be recovered at very high speeds back to a new or repaired server. The on-site appliance is in turn backing up to Iron Mountain's off site vault. The latter being crucial in order to comply with secure off line storage. The on site option provides another tier of service level to the customer and creates an extremely robust backup solution.

BACKING UP THE BACKUP

Iron Mountain have a mirrored server environment for all data stored. This in turn is also backed up to a tape robotic library. These tapes are then sent off site for secure storage. This means Iron Mountain provides a customer with an option for a copy of their data at their own location, a copy of the data at Iron Mountain's secure off site vault, this in turn is mirrored and then a tape copy is taken. Backing up the backup gives a very high level of protection for customer data.

CONCLUSION

Through the use of sophisticated replication technology, unique filter driver technology and database integrity algorithms, Iron Mountain's online backup solution, is able to provide a safe continuous backup solution. Iron Mountain's online backup solution frees the user from the headaches and errors (both technical and human) associated with a traditional backup. In order to achieve incredible reliability and simplicity for the user, a tremendous amount of sophisticated technology has been developed and deployed.

Should you require any further information please don't hesitate to contact us on 08000 27 27 20 or email our team on electronicvaulting@ironmountain.co.uk



Third Floor, Cottons Centre
Tooley Street, London
SE1 2TT, United Kingdom

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the UK, Europe, U.S, Canada and Latin America. For more information, visit our website at www.ironmountain.co.uk

© 2005 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated. All other trademarks are the property of their respective owners.