

Iron Mountain's Connected® Backup/PC Subscription Service Security Overview

CONNECTED BACKUP/PC SECURITY OVERVIEW

The majority of corporate data originates with PC users, often on laptops or home computers outside the firewall. Iron Mountain's Connected Backup/PC has the ability to capture and store this vital information regardless of where your corporate data is created — inside your firewall or out on the road — while dramatically reducing storage costs.

It is not enough, however, to back up the data. Even PC data that's being backed up and stored must be secured from outside threats. Iron Mountain meets this need with the data protection Subscription Service solution that truly and comprehensively protects the PC data that belongs to your organization. Iron Mountain follows rigorous standards to keep your data safe and away from others. Many of these standards are security best practices, while others were developed by Iron Mountain to reinforce these best-practice security measures.

The bottom line: Iron Mountain Inc. takes data protection very seriously, and has gone to great lengths to protect data from all credible threats. Iron Mountain specializes in off-site data protection and storage of PC data. Connected Backup/PC Subscription Service provides security at every level from backup through storage through data retrieval.

This document serves as an introduction to the security measures put in place within the Iron Mountain data protection architecture to prevent unauthorized access or damage to Iron Mountain customer data relative to physical access, via the Internet, via dial-in access, or by Iron Mountain employees.

DOCUMENT INFORMATION

Connected® Backup/PC Subscription Service Security Overview

PRINTED

February 2006

COPYRIGHT

Copyright © 2006 Iron Mountain Incorporated. All Rights Reserved.

TRADEMARKS

Iron Mountain, the design of the mountain, Connected, SendOnce and DeltaBlock are trademarks or registered trademarks of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.

Some software products marketed by Iron Mountain Inc. and its distributors contain proprietary software components of other software vendors.

CONFIDENTIAL AND PROPRIETARY INFORMATION OF IRON MOUNTAIN. The information set forth herein represents the confidential and proprietary information of Iron Mountain. Such information shall only be used for the express purpose authorized by Iron Mountain and shall not be published, communicated, disclosed or divulged to any person, firm, corporation or legal entity, directly or indirectly, or to any third person without the prior written consent of Iron Mountain.

DISCLAIMER

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of Iron Mountain Inc.. The information in this document is subject to change without notice and should not be considered a commitment by Iron Mountain Inc. While Iron Mountain has made every effort to ensure the accuracy and completeness of this document, it assumes no responsibility for the consequences to users of any errors that may be contained herein.

TABLE OF CONTENTS

	Page
What is Connected Backup/PC Subscription Service?	6
CONNECTED BACKUP/PC SUBSCRIPTION SERVICE: SECURITY	6
UNDERSTANDING KEY SECURITY ASPECTS OF CONNECTED BACKUP/PC SUBSCRIPTION SERVICE	7
Backup and Retrieve Session Security	7
Archival Security	7
Network & Firewall Security	8
Client Account Security	8
Administration Security	9
CONNECTED BACKUP/PC SECURITY INTEGRITY	9
The Iron Mountain Data Center	9
Connected Uptime – Mirrored Data Protection	10
Iron Mountain’s Backup Network	10
SUMMARY & CONCLUSION	11

ABOUT IRON MOUNTAIN DIGITAL

Iron Mountain Digital is the world’s leading provider of data backup/recovery and archiving software as a service (SaaS). The technology arm of Iron Mountain Incorporated offers a comprehensive suite of data protection and e-records management software and services to thousands of companies around the world, directly and through a worldwide network of channel partners. Iron Mountain Digital is based in Framingham, MA, with European headquarters in Frankfurt, Germany.

ABOUT IRON MOUNTAIN INCORPORATED

Iron Mountain Incorporated (NYSE:IRM) is the world’s trusted partner for records management and data protection services. Founded in 1951, the Company has grown to service more than 235,000 customer accounts throughout the United States, Canada, Europe and Latin America and the Pacific Rim. Iron Mountain offers records management services for both physical and digital media, disaster recovery support services, and consulting — services that help businesses save money and manage risks associated with legal and regulatory compliance, protection of vital assets, and business continuity challenges.

What is Connected Backup/PC Subscription Service?

Iron Mountain's Connected Backup/PC Subscription Service solution is a client-server system that enables file backup for personal computers over any TCP/IP network. Data is stored at a central server cluster managed by Iron Mountain Inc. at Iron Mountain facilities or at Iron Mountain Partner facilities.

The Connected Backup/PC Agent is a small, lightweight application that runs on every PC in an enterprise or business to manage backups and enable retrieval of data, scheduling and backup, and transaction logs.

Patented data reduction technology enables even large backups to take place in minutes. The software provides effective PC backup and recovery, even at connection bandwidths as low as 28.8 kbps. Connected Backup/PC Subscription Service provides a level of security for the user's data better than, or comparable to, alternative practices for handling computer data.

CONNECTED BACKUP/PC SUBSCRIPTION SERVICE: SECURITY

In the Connected Backup/PC Subscription Service client/server architecture, the client Agent is responsible for initiating backups; the Data Center servers are responsible for managing the data and keeping this data secure. The following sections illustrate how Iron Mountain creates a secure environment for data transfer, storage and manageability.

Iron Mountain's security objective is four-fold:

1. Prevention of unauthorized parties from gaining access to users' data during transfer over the Internet — **Backup & Retrieve Session Security**
2. Prevention of unauthorized parties from gaining access to users' data on the server — **Archive/Data Center Security**
3. Prevention of unauthorized parties from deleting users' data from the server — **Administrative/Client Account Security**
4. The physical security practices and building hardening that creates **Iron Mountain's Security Integrity**

UNDERSTANDING KEY SECURITY ASPECTS OF CONNECTED BACKUP/PC SUBSCRIPTION SERVICE

Backup and Retrieve Session Security

At the core of the Connected Backup/PC Agent is the backup engine. This piece of the Agent enables all backup and retrieval behavior at the client level. At the time of backup, the Agent scans the PC's disk, and determines what data to send to the off-site, highly available, mirrored Iron Mountain Data Center servers.

Backup is initiated when:

- The Agent contacts the Data Center via TCP/IP socket. SSL encryption (TLS 1.0) is used to protect user information during transmission.
- The server authenticates the Agent connection is authenticated via the user encryption key, while the Agent authenticates the server via a certificate embedded in the Agent install package.
- Following authentication, the Agent encrypts each file flagged for backup with AES [128-bit key] (or with older version Triple-DES [112-bit key] can be selected) and sends the data to the Data Center.
- The Data Center packs all the encrypted files from a given client's backup session into a single file on the server's file system, leaving the files encrypted.

Retrieve session:

- The Agent contacts the Data Center.
- The Agent then sends to the Data Center a list of files to retrieve.
- The Data Center transmits the encrypted files to the client, and the Agent decrypts them upon arrival and places them back on the client's disk.

A password option prompts the user to input a password prior to retrieval — using this password can prevent unauthorized persons with physical access to another person's client from performing retrieves from the server.

Archival Security

The data sent from the Agent to the Data Center is sent either in entire files or in deltas (changes to files previously backed up). Data is encrypted prior to transmission from the client PC. To prevent unauthorized parties from gaining access to users' data on the server:

- Iron Mountain encrypts all data with encryption algorithms.
- Data is encrypted using government-level, 128-bit, Advanced Encryption Standard (AES). (Triple-DES, 112-bit key encryption can be selected instead with Version 7.5 or earlier.)
- The encrypted output is sent to the Data Center. The Data Center stores the encrypted files without decrypting them.

It is important to note that the Iron Mountain Data Center is established as a storage repository and is not part of a communications system. The Data Center servers do not provide a view to user data. As a result, in the highly unlikely event that an individual is able to gain access to users' data files on the server, that individual would not be able to view the data.

Network & Firewall Security

Network Practices

The Iron Mountain Data Center Mirror:

- Is located at an undisclosed location.
- All data received by either Data Center is immediately replicated to its mirror.
- Outages or a disaster at either Data Center do not interfere with the availability of the data or the service.
- Iron Mountain has yielded 99.99% uptime for the past ten years, and most months are 100%.

Firewall Best Practices

Iron Mountain's firewall policies do not permit direct access from the outside to the Data Center file servers. Thus, access to customer archive files via remote connection to the production servers is not possible via the Internet. Iron Mountain uses a designated port that is only enabled for outbound traffic. For evaluation purposes, we also allow connections over port 80, but still using the same secure transmissions protocol (i.e., not HTTP).

Iron Mountain also employs intrusion detection systems.

File Retention

Iron Mountain retains the 10 most recent versions of any file backed up to the Data Centers, and keeps deleted files for 90 days.

To prevent unauthorized parties from deleting users' data from the servers:

- There are no commands that allow deletion in the client-server protocol.
- Administration has operational control mechanisms to prevent unauthorized access to Iron Mountain's servers.

Client Account Security

Each installation of Connected Backup/PC is unique to each customer. It is this ability to customize each deployment that enables Iron Mountain to maintain its lead in the PC data protection market. Data is transferred from PC to Data Centers on a daily basis. However, the administrator can customize administration rules and retrieval of accounts. This customization extends to the customer and their administration.

Visible/Invisible Keys (Version 7.5 and earlier only)

Recovery of an account requires an encryption key. Encryption keys have the option of being visible to select some, all or none of the administrative team, thus putting ownership of the data into the hands of the customer. It is for this same reason that Connected has an option to either escrow or not escrow all user encryption keys. Note that in version 8.0 and higher, encryption keys are never visible, and always randomly generated.

LDAP Authentication

Iron Mountain offers LDAP authentication for password-protected data retrieval via the Iron Mountain Enterprise Directory Interface (EDI). In this case, Subscription Service customers are authenticated via an HTTPS connection to a centralized database of usernames and passwords. Any challenge protocols to administrative credentials are initiated through the Iron Mountain EDI.

Ticketing

The ticket method uses a file (the ticket) that contains a single-use registration code. A ticket allows a single registration to the server and is usually provided in an email that accompanies the Agent Setup program.

User Account Security

File Security Descriptors (FSD) are employed to ensure that each user is only able to access the data associated with his/her account or an account to which they have been granted access. The FSD limits the client PC to only access its data, the data of a particular work group, or a department's shared folder. FSDs can be set to the folder level or the file level at the user PC.

Administration Security

Password Handling

When Connected Backup/PC users have questions or need assistance, they will typically contact the customer's Help Desk or similar IT organization. Support Center's features and data are protected against unauthorized access — every technician must present credentials when invoking Support Center.

Designated Help Desk technicians are supplied credentials authorizing their access to Support Center. Credentials consist of a Technician ID and an associated password. Only after the technician is validated with the proper ID and password, will access be granted.

CONNECTED BACKUP/PC SECURITY INTEGRITY

The Iron Mountain Data Center

Iron Mountain leases and controls all buildings which house its headquarters and mirrored, secure Data Centers. Iron Mountain manages its service with the goal of 100% uptime, 24x7x365.

Iron Mountain's Subscription Service is provided by a series of clusters which share a single registration server, each of which has one or more pairs of servers (mirrored). Mirrored servers are located at separate sites, which are connected by point-to-point, high-speed WAN links.

All Iron Mountain servers run Microsoft® Windows® 2000 or 2003 Server and SQL Server 2000.

Iron Mountain follows Microsoft best practices and implements security patches and database service packs when released, after acceptance testing.

In addition to deploying all the latest Microsoft security patches, Iron Mountain uses up-to-date virus protection to disable any virus attacks that threaten the Iron Mountain Data Center. As a result of our layered security model, Iron Mountain has not experienced any business interruption due to viruses or worms. It should be noted that since customer data is encrypted prior to arriving at the Iron Mountain Data Center, the virus scanning does not cover customer data.

Connected Uptime – Mirrored Data Protection

Iron Mountain's primary Data Center is located in two disparate locations. All data received by either Data Center is immediately replicated to its mirror. Outages or a disaster at either Data Center do not interfere with the availability of the data or the service. Iron Mountain has yielded 99.99% uptime for the past 10 years.

Most scheduled maintenance procedures and unscheduled outages affect only one member of a mirrored pair at a time. Mirroring practices enable Iron Mountain to service either side of the mirror without any business interruption. In the rare event that Iron Mountain must bring down both servers in a pair simultaneously, we will endeavor to do so outside normal business hours, with appropriate notification.

Iron Mountain's Backup Network

Internet traffic volumes can cause congestion at both the server and network levels. Connected created the concept of utilizing dual redundant mirroring to alleviate Internet congestion, giving customers access to multiple servers. Iron Mountain service runs on dual redundant mirrors in an active-active configuration, with load balanced between the two sites. Each agent has automatic fail over capability in the event of network outage. To further ensure access and performance, Iron Mountain utilizes high-speed Internet access lines to connect the Data Center servers to the Internet. The two data centers are linked by a high-speed connection for data replication and disaster recovery. Each data center has distinct ISP connections to provide redundant Internet connectivity. Servers are continuously monitored, and have 7x24x365 automatic event notification.

Hardening – Iron Mountain's Physical Security

Iron Mountain protects over 500 TB worth of PC data in its Data Centers worldwide. Access to these areas is restricted to Data Center Administrators only. Iron Mountain also takes the necessary steps to ensure that only Iron Mountain employees and signed-in guests of Iron Mountain employees can gain access to the Iron Mountain building.

- All Iron Mountain employees are issued a picture ID/card-key for entry to the building. Iron Mountain employees must display these Iron Mountain badges at all times. Card key use logs are reported and reviewed weekly.
- Access to the Data Center floor is further limited to Connected Backup/PC Operations team by biometric-controlled entry and is reviewed monthly.

Other Data Center Security measures include:

- Internal and external closed circuit television monitoring and recording.
- Internal and external alarm systems with 24x7 monitoring of motion detection, temperature, “waterbugs”, glass breaks, smoke and fire detection.
- Generator backup (tested weekly) with unlimited capacity to run on reserve power.
- Mirror data center is located within a locked cage at an undisclosed location with 24x7x365 security.
- Access to the mirror is restricted to pre-authorized individuals.
- Mirror is located on redundant power grids for increased availability in the event of a power failure.
- A dry fire-suppression system is installed at each site.
- Separate and distinct ISP to allow for further network redundancy.

SUMMARY & CONCLUSION

As of January 2006, Iron Mountain is managing over 500 TB (1 Petabyte with mirroring) of PC data at its Data Centers.

Iron Mountain has been backing up PC data since 1995, from enterprise corporate deployments for some of the world’s largest companies, to small businesses. Iron Mountain delivers the expertise customers need to reduce costs and risks associated with information protection and storage. Iron Mountain recognizes and acts on the fact that protecting intellectual property is critical.

It is for these reasons that Iron Mountain takes extreme precaution in handling customer data.

- Data is encrypted at the client PC prior to transmission for session security; data is unencrypted only after data restoration is completed to the client PC.
- Data is stored encrypted at secure, mirrored Data Center facilities.
- Iron Mountain operates its Data Centers with the understanding that downtime is not an option when considering a business-critical solution.
- Best practices networking and best-of-breed routers, switches, firewalls, servers, facilities infrastructure, power grids and telecommunications circuits are all deployed with Iron Mountain’s fail-over and redundancy technology to maximize service availability.
- Active mirroring assures that each client’s data has a duplicate copy at the mirrored data center to maintain client access in the event of failure at the primary location. This effort translates into the highest levels of security, and availability of 99.99%.

This document serves as a high level overview of Iron Mountain’s Connected Backup/PC Subscription Service.



Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, Latin America and the Pacific Rim.