

Achieving SaaS Security with LiveVault® Online Server Backup

Introduction

Today, more companies than ever recognize the value and convenience of using online backup to protect their server data. Enterprises considering online backup Storage as a Service (SaaS) face these security concerns:

- Could an unauthorized individual gain access to backed-up data?
- Could backed-up data be altered?
- Will necessary data be available when needed?
- Is data safe from fire, floods, and human error?

Iron Mountain Digital offers hosted data storage that enables customers to reduce the costs, risks, and complexity of storing and protecting their business information. With our heightened focus on security, privacy, and cost savings, Iron Mountain Digital goes beyond simple cloud storage to enterprise Storage as a Service.

LiveVault

Iron Mountain's LiveVault® service addresses all these concerns with the most secure solution available. For example, the LiveVault agent encrypts all data before transferring it from the customer's servers. All data remains encrypted at Iron Mountain's secure off-site Data Bunkers and on optional TurboRestore™ appliances. Only the customer controls the data encryption passwords. To ensure the physical security and availability of stored data, the LiveVault service employs a fully redundant vaulting infrastructure at two Iron Mountain underground Data Bunkers.

Iron Mountain also offers the LiveVault licensed product, which enables organizations to operate their own servers if they are concerned about allowing data to reside on Iron Mountain servers. Client-side security for the licensed product is similar to security for the Service. However, the security of stored data for the licensed product depends on the customer facilities, personnel, and policies.

Security for Data in Transit

The LiveVault service assures that the connection between application servers and Iron Mountain's secure off-site Data Bunkers is secure. The LiveVault service uses the best security methods available, including:

- *Automatic, outbound-only connections:* There is no added security risk to the customer's environment. In particular, there are no inbound connections. The LiveVault agent on a customer's server communicates only with the LiveVault backend infrastructure. The LiveVault agent initiates all connections from the customer's server (outbound connections) over two ports reserved for the LiveVault service, or over port 443 (the SSL port) if those ports are not available. Normally, there is no need to alter the firewall security perimeter. This makes installation particularly simple and secure at remote sites.
- *Public key encryption for mutual authentication:* The LiveVault backend infrastructure and the Agent software independently validate certificates each time a connection is made. This authenticates the Agent

to the electronic vault, and the vault to the Agent.

- *256-bit Advanced Encryption Standard (AES) encryption of all data before transmission and storage:* Your data is encrypted during transmission and remains encrypted at all times while stored at Iron Mountain. 256-bit Advanced Encryption Standard is the level of encryption that banks and government agencies employ.
- *Customers control encryption key passwords - escrow service available:* Customers may keep their encryption passwords private, so there is no possibility of any Iron Mountain employee accessing customer data. Iron Mountain also offers a free, optional escrow service for encryption passwords, which enables customers to recover data even if the encryption passwords are not available.
- *Customers can change encryption passwords:* If there is a potential security breach, such as when a trusted individual leaves a customer's company, the customer can simply change the data encryption passwords, which is similar to changing the door locks. Older backed-up data can still be restored, but only with the new password.
- *Digital signatures:* All communication between the LiveVault Agent and vault uses industry-standard SSL (Secure Sockets Layer). This prevents any accidental or malicious modification, and protects the integrity and confidentiality of all data.

Security for the LiveVault Web User Interface

The LiveVault Web user interface is convenient for customers to use because only a Web browser is needed for access from anywhere in the world. Security features of the Web user interface include:

- *Encrypted communication:* Secure Sockets Layer (SSL) encryption protects the LiveVault Web user interface.
- *Data protection:* The contents of backed-up files are not accessible.
- *Privacy protection:* Because data encryption passwords are not set or accessed with the Web user interface, even if someone steals a user's login and password, they cannot restore any data, except to the specific computer where it originated.
- *Strict password rules are available:* A company can set password specifications for their account, such as minimum password length, reuse policy, expiration period, and requirement for non-alphabetic characters.
- *Limits on insider attacks:* Customers can grant users only the rights and privileges necessary for their specific job duties. For example, a help desk person might have the ability to initiate restores, but not to set or change backup policies or add other users. Similarly, an IT administrator might have some (or limited) responsibilities for servers and users where they work, but not be able to see or manipulate servers or user accounts at other locations.

Entrance to an Iron Mountain underground facility.



Physical Security for Data Stored in Electronic Vaults

Iron Mountain owns or leases off-site Data Bunkers that provide high-security, environmentally-controlled storage for media, and includes data centers with redundant infrastructure. These Data Bunkers include data centers with redundant infrastructure.

These Data Bunkers include the following security measures:

- Extensive multi-acre underground sites.
- Gated entrances with 7x24 security guards.
- Restricted access requiring photo ID and visitor escort.
- Real-time closed circuit TV monitoring.
- Commercial power feeds with generators for full backup power.
- Clean Agent Fire Extinguishing System (CAFES) and on-site firefighting apparatus and personnel.
- Internal and external 24x7 environmental monitoring alarms for temperature, "waterbug" leaks, smoke, fire, and motion detection.
- External accreditation by the Uptime Institute according to their Tier Classification and Performance Standard.

The data centers within the Data Bunkers have achieved SysTrust® certification, which satisfies the specific Trust Services Principles and Criteria of the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). SysTrust examination assures that a system is reliable when measured against four essential principles: availability, security, integrity, and maintainability.

LiveVault Vaults

LiveVault data is stored in electronic vaults in each data center. When customers sign up for the LiveVault Service, their data is mirrored between vaults at each site for high availability. Iron Mountain constantly monitors the Data Bunkers, data centers, and vaults. In the unlikely possibility of a failure, backups are rerouted and continue automatically to the remaining vault. When the failure is repaired, all missing backup data replicates to the repaired or replaced vault. All other elements of the backend infrastructure, such as the Web servers, the backend database, and the command and control systems, are also redundant.

Storage Security

All data stored on LiveVault vaults (and on TurboRestore appliances or Media Restore Devices) is encrypted with 256-bit AES encryption. The only time data is decrypted is when a LiveVault software agent on a customer's server receives encrypted data while processing a restore request.

Secure, Reliable Server Protection

Strategic partners, including IBM, HP, and LexisNexis, have selected the LiveVault solution to protect their customers' valuable data. Today, over 13,000 servers worldwide are under the protection of the LiveVault Service.

Data backed up with the LiveVault Service is automatically off-site and safer than it is in the customer's own facility. Customers rely on Iron Mountain to have their data available when they need it, while protecting the privacy and integrity of the data.



©2009 Iron Mountain Incorporated. All rights reserved. Iron Mountain, the design of the mountain, and LiveVault are registered trademarks and Iron Mountain Digital and TurboRestore are trademarks of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.

120 Turnpike Road
Southborough, Massachusetts 01772
(800) 899-IRON

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, Latin America, and the Pacific Rim. For more information, visit our Web site at www.ironmountain.com.