

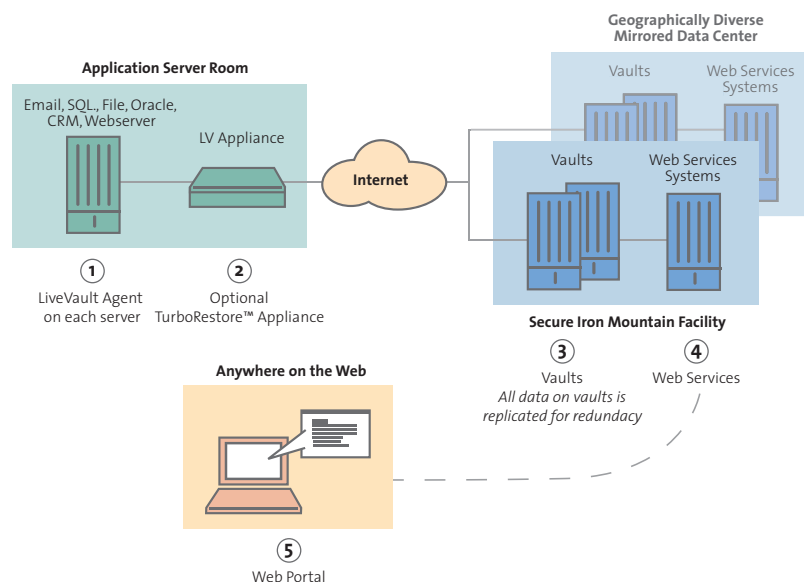
## LiveVault® Components

### EXECUTIVE SUMMARY

LiveVault eliminates the hassle and expenses related to traditional tape-based backup solutions, and provides significantly better reliability by automating the backup process, thus reducing the opportunity for human error and oversight. As a premier online backup solution, LiveVault also provides a rich set of features such as 15 minute roll-back granularity, flexible retention settings, a Web portal, state-of-the art security that encompasses much more than data encryption and an optional local appliance, TurboRestore™, for faster restores.

The underlying technology consists of five major components:

1. **Agents** – The agent software resides on customer servers and is responsible for securely backing up and restoring a server's data.
2. **TurboRestore Appliances** – Appliances are optional local caching devices that sit in the data path between agents and vaults. They provide for faster restores and flexibility of backup schedules to allow trade-offs between backup frequency and bandwidth use.
3. **Vaults** – Vaults are the primary repository for customer backed up data. Vaults provide defined retention for backed up data and secure, redundant storage at two geographically diverse locations.
4. **Web Services** – “Web services” is a generic name to refer to the set of services that provide the control, communications and management infrastructure for the LiveVault service.
5. **Web Management Portal** – The Web UI is the primary interface for customers. From this secure portal, customers have access to all appropriate backup, restore and reporting/monitoring functionality for their data protection.



# Table of Contents

Agents .....	3
Appliances .....	5
Vaults .....	7
Web Services .....	8
Web Portal .....	10

## AGENTS

The LiveVault agent has four primary functions: 1) data capture, 2) data transfer, 3) data restore and 4) status reporting. The LiveVault agent works at the file system level. Specific drive letters, directories and/or individual files can be included or excluded from backup policies. Unlike incremental tape backups, the agent performs delta backups and restores in which only new and changed file system blocks are transmitted.

During the installation of the LiveVault agent, the administrator specifies a data encryption password for the server. This password is needed to do a full system disaster recovery and to do a re-directed restore onto a different server. Just like locks on the door, the data encryption password can be changed anytime there is a concern that it might be compromised.

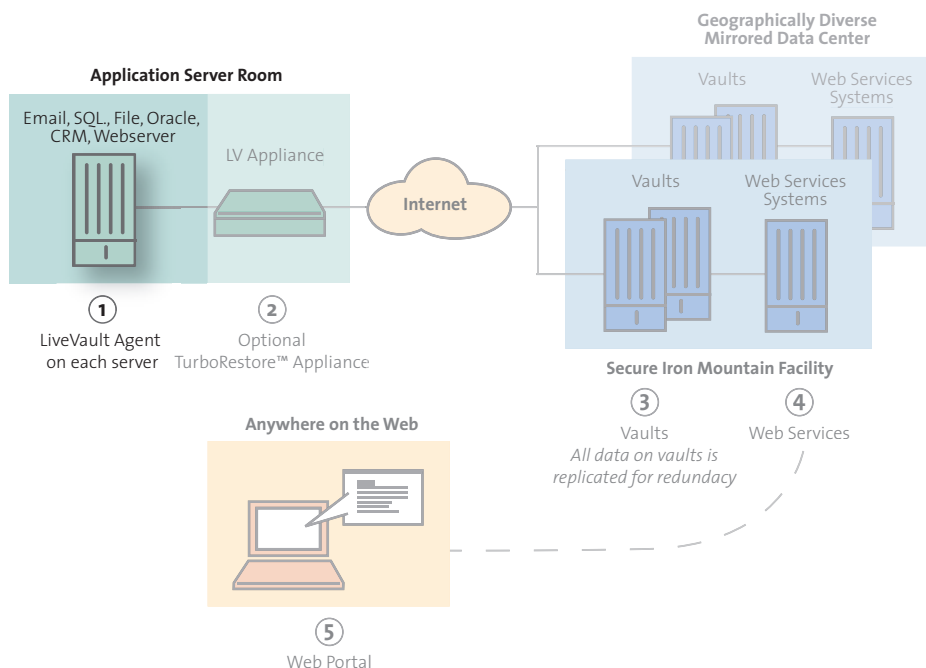
After setting up LiveVault on a system and creating one or more backup policies, the agent sends an encrypted copy of all the blocks of all files that have been selected for protection. From this point on, only the blocks that change or are created are sent from the agent. The combination of delta backup (just changed or new data) and compression ensures that bandwidth is used very efficiently.

For Windows® servers the agent has unique technology that allows backups to occur as frequently as every 15 minutes with no noticeable performance degradation. There are two stages in performing a delta backup, (a) identifying what the new or changed blocks are since the last backup, and (b) compressing, encrypting and transmitting those blocks. In addition there is the concern that the backup not interfere with ongoing database and other activity on open files. The LiveVault agent starts a backup by taking a snapshot. This provides it with a static, read-only image of the on-disk state at the instant the “freeze” command was issued. (On Windows 2003 and later the agent uses Microsoft® Volume Shadow Copy Service (VSS) to make the snapshots). Using a snapshot means that there are no locked files, no problems accessing open files and databases.

With the snapshot image in hand the agent’s next challenge is to identify what blocks have been created or changed since the last backup. Here the agent has a unique advantage. One component of the agent is a filter driver that is installed into the file system itself. This “driver” records all the write activity that occurs, so each time the agent needs to perform a backup it can consult the list made by the filter driver. The agent knows immediately what data needs to be transmitted. There is no overhead required to check file last modified dates, or do checksum comparisons on data blocks. On large servers or servers where there are large open databases, the resource load (primarily disk I/O) to scan for changed data would be noticeable and burdensome, effectively restricting the frequency with which backups would be practical from a performance standpoint.

The use of snapshots has an important implication for database backup and recovery. The agent is optimized to have a maximally efficient backup process, so that backups are practical 96 times a day, 4 times an hour. Therefore LiveVault defers the problem of transactional integrity from time-of-backup to time-of-restore. Modern databases use transaction logs and other techniques to ensure proper recovery after a server outage, such as power failure. That is, when the database starts up, it examines the state of its various files and if necessary rolls back incomplete transactions to establish transactional integrity. After restoring a database from a LiveVault backup, the database software will see exactly what it would have seen had there been a power outage at the time the snapshot was originally taken, and the database will do its normal recovery processing if necessary. This means that agent’s backup process does not burden databases or other applications with required lapses in full service or performance; the two are independent.

Because Microsoft Exchange is a critical database application the agent does have a special ability to backup Exchange 2003 in an “Exchange-aware” manner. This is a LiveVault option. If an Exchange-aware backup policy is selected, then the agent informs Exchange of an impending backup before the snapshot is taken (through a Microsoft facility known as a VSS writer). This causes Exchange to flush its buffers and come to a transactionally consistent state so that when the snapshot is taken and backed up, the backed up files are in a known good state that will not need any recovery processing if later restored.



The agent makes two outbound TCP connections (no inbound connections are needed). The first connection is to the backend “bridge service.” The agent must be able to resolve the name bridge.livevault.com. Over this connection the agent gets its instructions (what the backup policies are) and what vault or TurboRestore Appliance (TRA) it should talk to. It then makes a second outbound connection to the designated vault. Over this connection backed up data and restored data will flow (connection establishment is always outbound; once the connection is made data can flow in both directions). All connections are mutually authenticated through the use of public key encryption (PKI) certificates. At the time the agent is installed it must also be able to resolve the name provisioning.livevault.com to register its certificate, and it will renew its certificate on six month or yearly intervals.

Using checkpoints in all data streams, LiveVault is able to recover from any type of communications or device failure without having to resend entire jobs — picking up from where it left off. This is also true of TurboRestore Appliances and vaults.

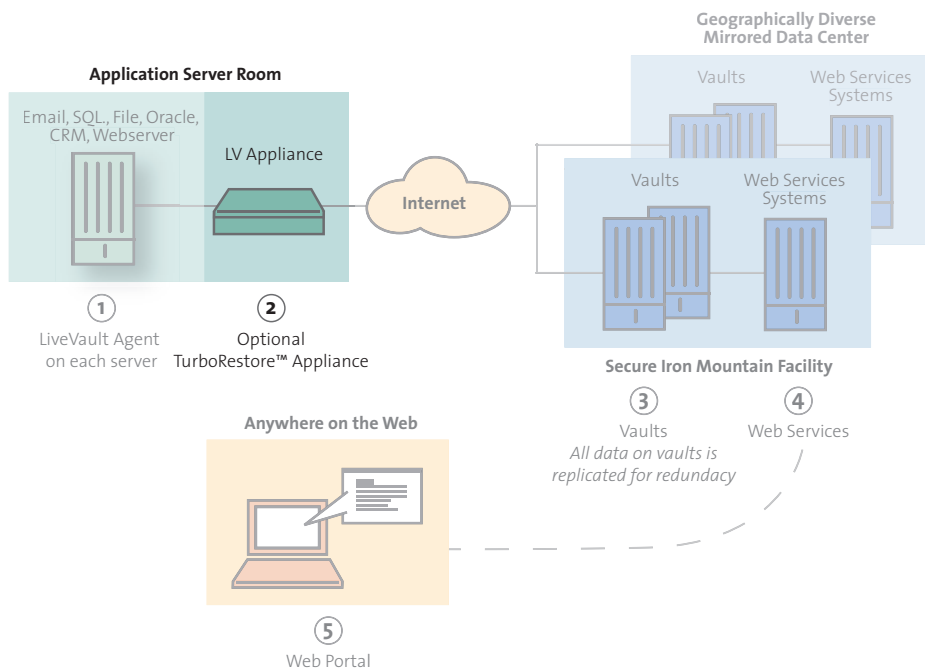
LiveVault operates on the concept of guaranteed backup jobs. This means that LiveVault finishes a backup job before it starts the next one. If the agent is still sending data when the time comes to start the next backup job, the agent will continue with the on-going backup and will skip the backup job that was to start. As a result, servers using continuous protection where the agent makes a “best effort” to perform a backup every 15 minutes may have fewer than 96 backups completed on a busy day, but the backup process will not get behind in the event of a large data change event. This is true for communications between agents and TurboRestore Appliances and agents and vaults.

In addition to this agent-side mechanism, unlike traditional backup technologies that restore whole files on restore, LiveVault only restores the changes or deltas to the file whenever possible. The most common reason for restoring a file or database is some type of corruption event, typically some type of human error. In such cases the LiveVault agent automatically uses its delta technology “in reverse” — restoring only the blocks of data that are different. For restores of larger files, particularly database files, this can save considerable amounts of time.

In addition to the core data movement and communications technology, the LiveVault agent also sends status on an ongoing basis to the Web Services, which are then able to provide information to the Web portal for reporting and analysis.

**APPLIANCES**

LiveVault offers an optional onsite device, TurboRestore Appliance, to allow customers to have locally cached copies of all or some of their backup data for faster, local restores in addition to having the data stored offsite in Iron Mountain’s secure facilities.



Appliances are relatively inexpensive hardware units running an embedded version of Microsoft Windows® 2003/XP with specialized LiveVault TurboRestore software. Appliances typically have about two times as much storage as the data being protected. This allows the appliance to hold several weeks of backup history and to have temporary space for its operations. On appliances, historic versions of customer data are maintained for a couple of weeks or so (depending on the relative capacity of the appliance to the amount of data being protected). By contrast, vaults (discussed later) maintain historic versions of data based on customer defined settings, such as 30 days, 1 year or 7 year retention.

Appliances are designed to be plug and play simple, with virtually no local maintenance or setup required. If there is a failure of the device, it can be replaced with minimal service disruption. Additionally, appliances are entirely optional in the chain of data flow — if an appliance has a failure, backups can easily be rerouted directly to vaults, by disabling the appliance in the Web-based user interface.

All data that is stored on appliances or vaults is encrypted and compressed, so it is both efficient and secure.

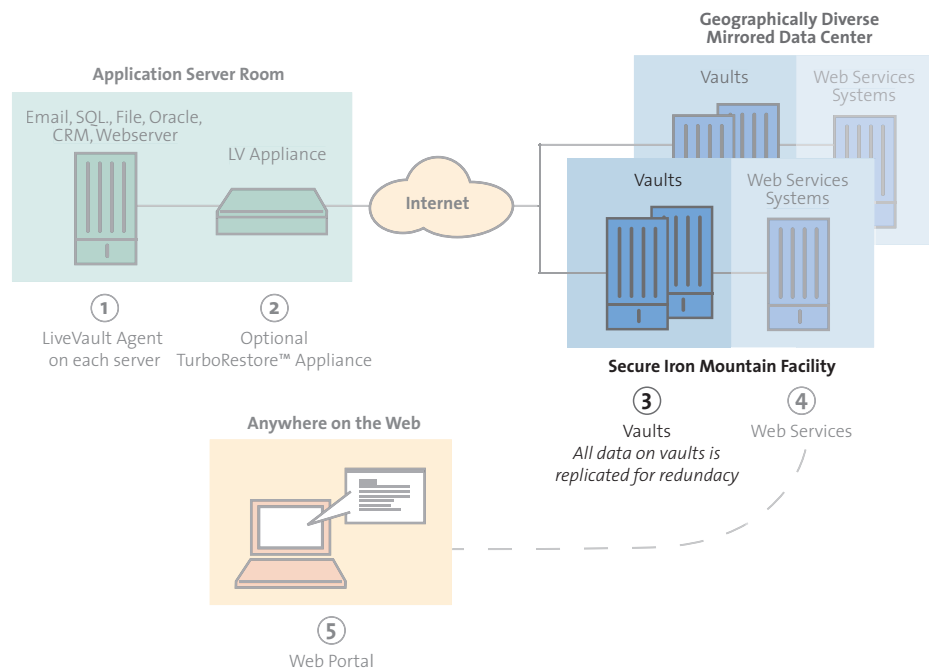
When restores are initiated, LiveVault automatically determines the “closest” location of the data to the machine being restored to. For example, it will determine if the data is stored on a local appliance first, then if not find it on a vault.

TurboRestore Appliances (and vaults) use a LiveVault process called coalescence which allows agents and appliances to compress iterative changes to the same blocks into the difference between their previous backed up state and their current state. In other words, if an appliance takes more than 15 minutes to get its backup job offsite, it will then combine all the changes of the backup processes that were missed into one compacted backup set. This is the same process that vaults use to maintain less granular versions of historic versions — such as month-end copies. In this case, LiveVault is able to condense all the daily backup changes down to just the differences between the beginning and end states — for much more efficient storage of data.

## VAULTS

Vaults are the repository for customer information. Unlike appliances that typically have limited fault tolerance and redundancy, vaults have high levels of both, with at least one replicated version of all data on an entirely different piece of hardware at a separate Iron Mountain vaulting facility. Additionally, vaults store data based on defined retentions. All retention policies retain all backups for at least one day. With continuous protection this means all of the 15 minute versions will be available for the most recent 24 hours. For the most recent week, LiveVault retains four versions per day, and daily versions for the remainder of the 30 day retention period. After 30 days, customers with longer term retention can have month-end versions for 12 months and calendar quarter-end versions for up to 7 years.

Vaults, like appliances, store compressed, encrypted versions of blocks of customer data. The data is stored in vaults organized by policies, which are specific backup jobs on particular protected customer servers.

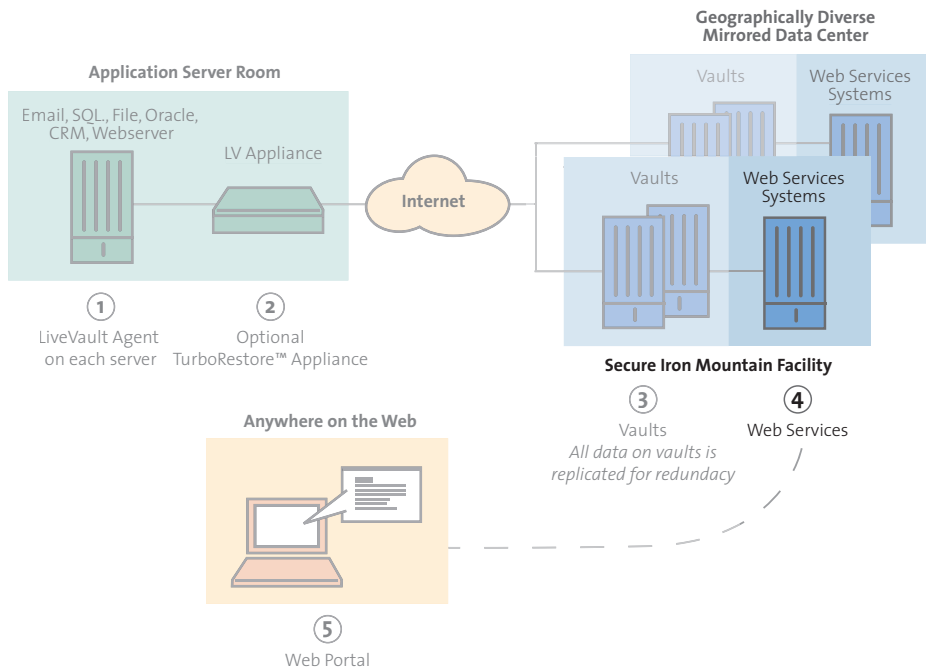


**WEB SERVICES**

The LiveVault Web Services are a number of components that work together to provide the back-end infrastructure required for the LiveVault Service to operate. These services include communications routing, collecting data for reporting, encryption key escrow and policy management.

A unique LiveVault feature is the ability to move servers to different logical or physical locations without having to reconfigure the systems. All protection nodes (agents, appliances and vaults) maintain a persistent connection to the Web Services (calling out through outbound connections). The Web Services then track the location of those nodes and share that up-to-date information with the other nodes that need the information. As a result, each protected node always knows the location of the other nodes it talks to, regardless of where they are or if they have recently moved.

The Web Services collect the data that is reported in backup logs, restore logs, audit logs and bandwidth usage charts.



Security is a challenging problem with respect to backup data. On one hand, customers want to have quick and easy access to their information when they need it for restores or recoveries. On the other, they want to ensure that the data is secure as it travels and is stored. Most solutions address these challenges with customer-defined and controlled encryption keys. With this approach, only the customer who creates the key and whoever that person gave the key to have access to the key. Because it is very complex and difficult to decrypt and re-encrypt data, the original key is generally THE key for the life of the data stored with the system. There are two problems with this approach. First, if the key is lost, the data is lost — because in this model, only the customer has the key. Second, if the key is compromised, the data is compromised. The key generally cannot be changed, so either the data has to be destroyed or the risk of a compromised key assumed.

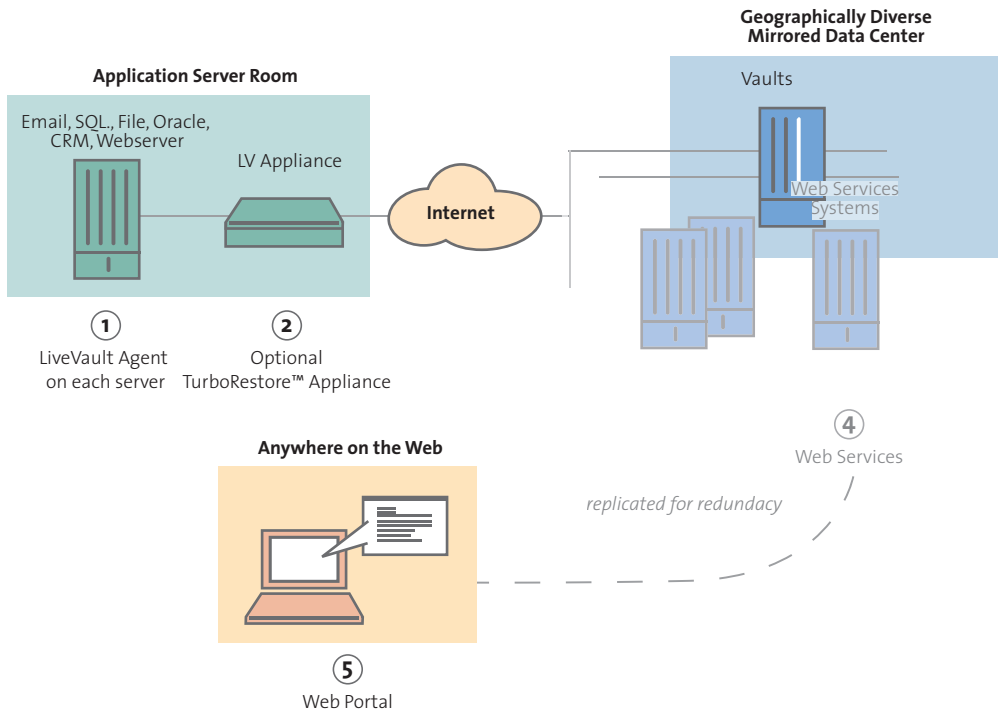
LiveVault has a new approach to encryption key management that offers two unique features. First, customers have the option of escrowing their passwords with Iron Mountain. Second, customers can change a password at any time. The old password becomes completely ineffective, yet the previously backed up data does not need to be re-encrypted. These key management features are particularly valuable for servers with a long life span and for backups that need to be retained for a long time under the 1 year or 7 year retention plans.

The Web Services component provides policy management. In LiveVault, policies are sets of instructions that define either backup specifications or restore requests. If an agent or TurboRestore Appliance is disconnected for a period of time (such as in the case of a re-boot), when the LiveVault service is able to connect again to the Web services, it will check for the current state of all pertinent policies.

**WEB PORTAL**

The Web portal uses bi-directional SSL security for all communications. From a security perspective, there are two important features that are available through the interface. First, customers can audit all jobs and user activities associated with LiveVault. Customers can view who made what changes to settings or initiated what jobs and the details of those changes. Second, larger customers can specify the specific rights and privileges and span of visibility of each user. Individuals can be limited to managing and/or viewing specific systems.

Customers use Internet Explorer (or other browsers) to perform all functions relating to backup, restore, reporting and user management. The Web portal provides customers with the ability to control exactly what data should be backed up or restored, the schedule and how much bandwidth is acceptable. The only functions that are not part of the Web interface are related to software installation (initial install is done locally) and encryption password management.



This page intentionally left blank.

© 2009 Iron Mountain Incorporated. Iron Mountain, the design of the mountain, Iron Mountain Digital, LiveVault and TurboRestore are trademarks or registered trademarks of Iron Mountain Incorporated in the U.S. and other countries. All other trademarks and registered trademarks are the property of their respective owners.

 **IRON MOUNTAIN** DIGITAL™  
120 Turnpike Road  
Southborough, Massachusetts 01772  
(800) 899-4766

Iron Mountain Digital is the world's leading provider of Storage-as-a-Service solutions for data protection and recovery, archiving, eDiscovery and intellectual property management. The technology arm of Iron Mountain Incorporated offers a comprehensive suite of solutions to thousands of companies around the world, directly and through a worldwide network of channel partners. Iron Mountain Digital is based in Southborough, MA.