

Secure Transmission Over the Internet

Growing numbers of businesses are recognizing the value and convenience of using Internet-based online backup. Yet, many have lingering questions about data security, especially transmitting proprietary, confidential data over an inherently public network such as the Internet. If you are a Network Administrator, CIO, or small business owner considering LiveVault online backup, recovery and electronic vaulting managed services, you may be wondering:

- *How secure is my data during transmission over the Internet?*
- *How can I be assured that my data is protected from being viewed or stolen by unauthorized users or compromised by hackers?*

LiveVault Online Backup Service addresses these concerns with state-of-the-art security technologies similar to the ones which major financial institutions use to protect their confidential financial transactions. In particular, LiveVault combines password-protected SSL-level web access, electronic key technology, advanced encryption techniques, and industry standard digital certificates with proprietary Virtual Private Network (VPN) tunneling technology to produce a highly secure passage for data and guarantee the authenticity of sites sending or receiving data over the Internet.

Secure Access to MyLiveVault™ Security is built in from the very beginning. The first step in subscribing to LiveVault entails visiting MyLive Vault, your own web management interface for LiveVault. When accessing MyLiveVault—whether to enroll, download or install LiveVault Agent software, set backup policies, or initiate restore operations—your connection is secured with Secure Socket Layer (SSL) and login protection. To ensure the maximum level of security using SSL, you must use a browser that supports 128-bit encryption. This is the same level of security that is used today for secure online transactions with banks and e-commerce sites. It is also the same level of security that most business-to-business sites use.

Establishing an SSL connection ensures that you are connected to the web page you intended to connect to. You will be prompted to enter a username and password so that LiveVault can verify that you are who you say you are. The SSL connection is like a secure tunnel with one-way authentication. You are assured of the identity of the site you are connected to, and LiveVault knows who you are when you identify yourself by logging in with your username and password.

Digital Certificates A digital certificate is an electronic identity issued by a trusted third-party, called a Certificate Authority, who, in effect, verifies your identity. When you sign up for LiveVault Service, LiveVault creates and issues digital certificates that individually identify each protected server. The LiveVault Internet Gateway and backup servers that receive your data also have their own unique digital certificates. These digital certificates enable a customer server and its associated LiveVault servers to authenticate their identities to each other and to certify that they are to be trusted before they exchange data. Only after such two-way authentication is established does the LiveVault Internet Gateway create the VPN tunnel for exchanging data. Since only a LiveVault Agent with a valid certificate can communicate with a LiveVault Internet Gateway server, it is virtually impossible for an unauthorized user to make a connection from any computer other than a protected server.

The basic components of a digital certificate are: name, electronic key, and signature. Electronic keys are essentially very large, 1024-bit numbers that are used to encrypt data. Keys may be public or private and are used in pairs. Public keys can be disclosed to a selected party. Private keys are kept to yourself. You can encrypt a piece of data with the public key and then send that data to a designated recipient. Using the other (private) key in this pair, the recipient can then decrypt it. So by encrypting data with a shared public key, you ensure that only parties who have the matching private key can “unlock” the data.

When you use LiveVault Online Backup Service, you become part of LiveVault’s extended network. LiveVault controls every node on this network, decides who has access, and issues digital certificates to every authorized user. Each standalone LiveVault Internet Gateway server has its certificate. Nobody else can create a certificate that both you and LiveVault can trust. Since LiveVault is sharing a network connection with you, you can trust that we are protecting our own data as well as yours.

VPN Tunnel Technology LiveVault digital certificates authenticate the identity of all networked servers, so that the LiveVault Internet Gateway can then establish a Virtual Private Network (VPN) tunnel that will transmit data between a client’s server and the Iron Mountain data center.



LiveVault VPN tunneling technology uses encryption and signing to create a private connection over a public network. This VPN technology, in effect, converts public networks, such as the Internet, to private networks that can be accessed only by authorized personnel. The tunnel is a way of putting data inside a protected container. It can be described as a secret envelope that's wrapped around all your data, or like sealing data in a safe and sending it to someone who has the key and knows how to reopen the safe. Even the network addresses are encapsulated in this envelope. LiveVault ensures that only authenticated backup and restore traffic will enter or leave through the VPN tunnel created between two authenticated servers. This is the same technology that major financial institutions use for their Internet-based transactions.

Once the VPN tunnel is established between two servers that have granted each other mutual trust, all data that is sent through the tunnel is protected by the Advanced Encryption Standard (AES) and a digital signature. AES is a state-of-the-art encryption standard developed by the U.S. National Institute of Standards and Technology (NIST) with industry experts and the cryptographic community. The overall goal of AES was to develop a Federal Standard that specifies an encryption algorithm(s) capable of protecting sensitive government information well into the next century.

Before data is sent over the network, AES encryption is used to encode it with a session key that is only shared with the LiveVault server at the other end. For maximum security, all data elements, the headers, and network addresses are also encrypted. So even if someone could gain access to what is inside the tunnel, they would still not be able to identify the owner of the data or its source address.

Besides being encrypted, data going through the tunnel is also signed and compressed. Signing provides another level of data security. A digital signature on encrypted data confirms that the data has not been intercepted, decrypted, and re-encrypted before it is received. For additional security, the session key used to encrypt the digital signature is changed or "refreshed" periodically. In the VPN tunnel, data is also compressed to maximize speed and efficiency in use of available bandwidth. LiveVault VPN tunnel technology compresses data before encrypting it for optimal cost effectiveness.

A Complete Internet Security Package When deciding whether to use an Internet-based electronic vaulting service, data security is a valid issue that must be addressed. You need to know that your data is protected from loss, from tampering or theft, and from unauthorized access during its network journey from your protected servers to the LiveVault servers in the Iron Mountain data centers. LiveVault Online Backup Service addresses this issue with state-of-the-art security technology.

LiveVault Internet security combines password-protected SSL-level web access, electronic key technology, advanced encryption techniques, and industry-standard digital certificates with proprietary VPN tunneling technology to produce a secure passage for data and guarantee the authenticity of sites sending or receiving data over the Internet. LiveVault's VPN tunnel alone provides three layers of security:

- *The tunnel can only be established between two servers whose digital certificates allow them to authenticate each other*
- *Encrypted data inside the tunnel is virtually invisible, completely protected from anyone that does not have the key to decrypt it*
- *Signing provides additional assurance that transmitted data has not been tampered with*

LiveVault Online Backup Service guarantees that your data is fully protected.



www.livevault.com
LiveVault Corporation
201 Boston Post Road West
Marlborough, MA 01752 USA

