Cloud Backup Security Overview

April 21, 2015

No IT professional questions the necessity of data backup, but you want to know your data is absolutely secure before, during, and after the backup process. Unlike legacy tape-based solutions—which are vulnerable to theft, disappearance, and deterioration—the powerful, reliable security model employed by the VaultLogix cloud backup and recovery solutions guards against data loss and leakage from beginning to end.

Key Benefits

- Military-grade, end-to-end encryption protects your data every step of the way
- Controlled data access means you alone own the encryption key, and the VaultLogix data center cannot access your system

Encryption

End-to-end encryption: With the VaultLogix solutions, your data is encrypted through every step of the backup process—from the source server through data transmission and while in storage.

- **Start at the source:** Before your data leaves the server, it's protected at the level you choose: 256-bit AES (Advanced Encryption Standard), 128-bit AES, 112-bit 3DES, or 128-bit Blowfish encryption.
- **Over-the-wire encryption:** As your data travels over the Internet to the vault, you can relax knowing it's protected by 128-bit AES encryption. Because VaultLogix's deduplication ensures you back up only new or changed blocks, you simply expose much less data during the actual backup.
- **At-rest encryption:** Finally, your data stays safely encrypted while in the VaultLogix top-tier rated and SSAE (Statement on Standards for Attestation Engagements) 16-compliant data centers.

FIPS-approved AES encryption: You deserve the assurance of knowing VaultLogix encryption is certified by NIST (National Institute of Standards and Technology) as specified by FIPS (Federal Information Processing Standards) Publication 197. FIPS 197 designates AES as the standard for encrypting data used by federal departments and agencies. FIPS-approved encryption modules comply with that standard. We're committed to meeting or exceeding regulations and standards that enable us to deliver the high level of security you need and expect from us.

You alone control the encryption key: The VaultLogix solutions have no "back door" decryption keys: once you establish your encryption password and settings, no one else can access or decrypt your backup data—not even the VaultLogix employees who manage your data at an offsite vault. In information security circles, this is known as a "trust no one" security paradigm. At VaultLogix, we call it "business as usual."

Authentication and Authorization

You're in control from the moment you initiate the backup through communications and management. Both authorization and authentication are required to begin every backup and restore session, so you know each one is completely cleared and approved. Your VaultLogix solution will identify and validate the system, the account, and the username and password used to access the vault; the authentication information itself is encrypted for security. Any interaction between your systems and the vault must be initiated on your end. When data is pushed out to a secure data center during a backup and restore session, there are no inbound connections to your network—and no concerns about unauthorized access.

Communications are also locked down when you're managing your backup processes. The VaultLogix solutions encrypt interactions with the management portal, so you can configure your backup jobs and policies without compromising the security of your systems.

VaultLogix's role-based security model enables you to flexibly control access to the system. Various options let you choose who has the ultimate power to restore, encrypt, and decrypt data, or perform other backup and restore related functions.

Operational Controls

Operational security: You can easily track backup and restores using detailed logs that create paper audit trails. Rest assured that procedural, electronic, mechanical, and physical controls are protecting the physical security of the VaultLogix data centers:

- Key-card and/or biometric access
- 24/7 surveillance cameras
- Background checks on all employees
- Data center access limited to authorized employees only