

Advanced end-to-end Security

The trusted technology in online backup and recovery provide peace of mind to over 20,000 businesses worldwide

Recent - and mounting - headlines announce that companies large and small have experienced data theft, including credit-card and other sensitive customer information. Tape-based backups are vulnerable to theft because of the manual handling involved and are typically not encrypted (if even available) because the encryption process can be time-consuming. Continu Vault removes the human-element and threat of exposure through data-centric technologies of Delta processing, compression, and encryption to create a powerful and reliable security model. NIST validated AES encryption

The National Institute of Standards and Technology (NIST) created the Federal Information Processing Standards (FIPS) Publications 197 specification as the standard for testing AES encryption technology. Companies that are FIPS Certified meet the communications Security requirements for AES data protection and compliance. Continu Vault Enterprise's AES encryption technology is fully FIPS Pub 197 certificated.

Key Benefits

End-to-end protection of mission critical data

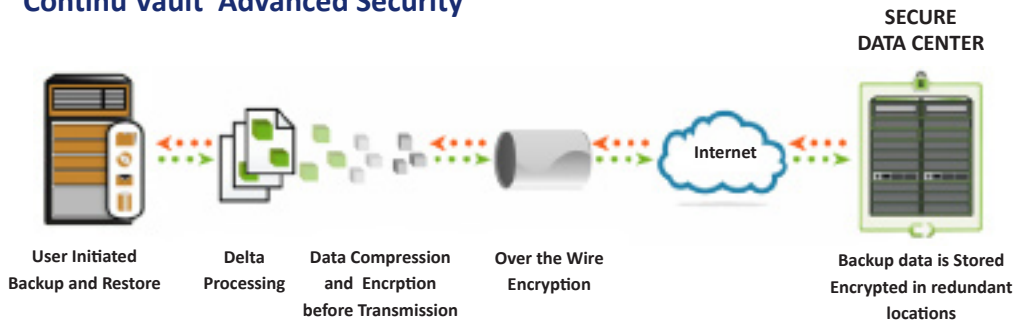
User controlled, flexible configuration

Peace of mind knowing that company data is secure and backed up offsite

Superior reliability and performance

Secure data center facilities

Continu Vault Advanced Security



Data is compressed and encrypted during backup (or unencrypted and decompressed during restore) on the client's local systems before it leaves the firewall and remains encrypted during transmission and storage in Continu's secure data centers.

User initiated connections only

All interactions between the client systems and the electronic vault are initiated by the client system. Data is pushed outbound to one of Continu's secure data center facilities. No inbound connections into the client's network are made during either backup or restore session. There is no entry attempt from a foreign source through the client firewall.

Strong data encryption

Continu Vault offers multiple, user defined encryption levels. Higher levels include 256 bit AES, 128 bit AES, 112 bit 3DES, and 128 bit Blowfish. Data remains encrypted throughout transmission and while in storage and is only deciphered upon restore with the help of a user-defined password key. Not even Continu personnel have access to this password key.

Secure over-the-wire encryption

The backup and restore activity is encrypted. This "over-the-wire" encryption, assures that transmission of backup data between the client and the electronic vault is secure, even when using the Internet.

Authentication, Authorization, and Accounting

Continu Vault requires that each backup and restore session is both authorized and authenticated before data transfer can commence. The vault will uniquely identify and validate the system, the account, and the username and password used to access the vault. All of the authentication information is always encrypted. All backups and restores are tracked in detailed logs.

Delta processing

Continu Vault's Delta Technology speeds up backup operations and drastically reduces storage costs as only new and changed data blocks within a file are backed up. All backup data can be compressed and encrypted before being transferred and remains that way on the storage vault, increasing security. Continu Vault delivers superior performance that optimizes backup and restore functions, lowers backend storage costs and helps businesses to gain and maintain regulatory compliance.

Optimized data compression

Continu Vault employs patent pending advanced, user configurable data compression techniques. By combining compression encoding along with sophisticated encryption algorithms, data security is inherently increased. Data remains compressed through transmission and while in storage to optimize bandwidth usage and to reduce client storage costs.

Secure data center facilities

All customer data is stored on state-of-the-art fully redundant hardware and is proactively monitored around the clock. In order to enter the vaulting facilities, personnel are required to meet security clearance and must pass biometric verification. The facilities employ 24-hour video monitoring and climate/humidity monitoring to ensure full protection of the hardware and data. Each data center is supplied with redundant power and Internet connections.