

Technical Brief

Delivering Advanced Online Backup End-to-End Security

The trusted experts in online backup and recovery provide peace of mind to over 7,000 customers 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. VAULT400 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 Technologies (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. VAULT400's AES encryption technology is fully FIPS Pub 197 certificated.

The importance of SAS 70 compliance

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

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 off-site

Superior reliability and performance

Secure data center facilities

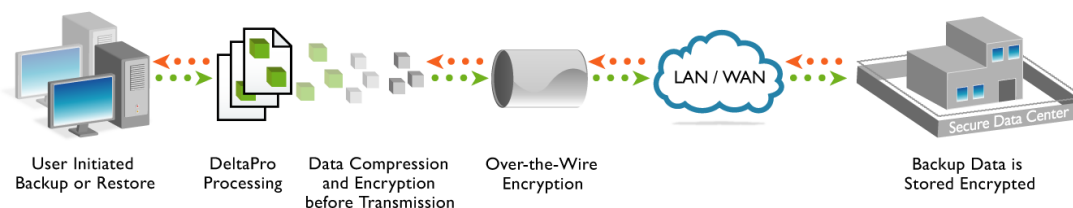
North America

United Computer Group Inc
Alpine Center
7027 Mill Road #206
Cleveland, OH 44141-1813

Office: 440-717-7655
Facsimile: 440-717-7662
Toll-Free: 800-211-8798

VAULT400 Advanced Security

CLIENT SYSTEMS



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 VAULT400's secure data centers.

www.ucgrp.com
www.vault400.com

VAULT400 is a licensed solution of United Computer Group, Inc. August 2006

Advanced Data Security Features

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 VAULT400'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

VAULT400 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 VAULT400 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

VAULT400 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

VAULT400's patent pending 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. VAULT400 delivers superior performance that optimizes backup and restore functions, lowers back-end storage costs and helps businesses to gain and maintain regulatory compliance.

Optimized data compression

VAULT400 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

For VAULT400 Protect customers, VAULT400's secure Tier-1 data centers are constructed to carrier-class specifications. All customer data is stored on state-of-the-art fully redundant hardware, continually backed up, and 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 security and climate/humidity monitoring to ensure full protection of the hardware and data. Each data center is supplied with redundant power and Internet connections and includes fire and earthquake protection.

