

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

Data backed up to two geographically separated data centers

Secure data center facilities

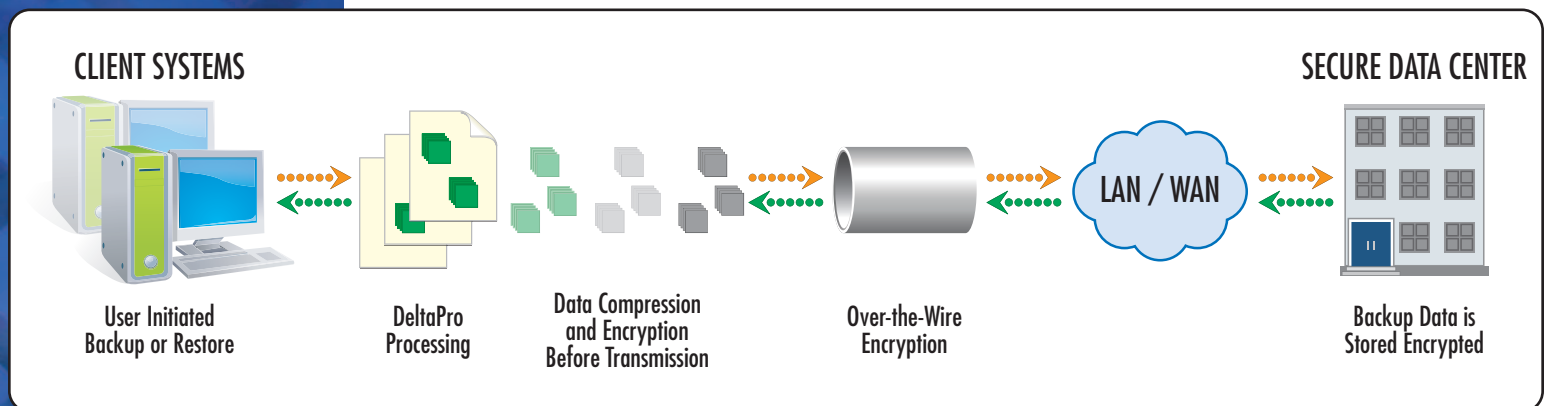
DataGuardian™ Advanced End-to-End Security

The trusted experts in online backup and recovery provide peace of mind to hundreds of clients worldwide

Recent - and mounting - headlines announce that companies large and small have experienced data theft, including credit-card and other sensitive employee or customer information. Tape-based backups are vulnerable to theft because of the manual handling involved and they are typically not encrypted because the encryption process can be time-consuming. DataGuardian removes the human-element and threat of exposure through data-centric technologies using 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. DataGuardian AES encryption technology is fully FIPS Pub 197 certificated.

DataGuardian Advanced Security



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

IPR International, LLC

8 Tower Bridge
 161 Washington St • Ste 800
 Conshohocken, PA 19428
 PH 484.533.6800
 www.iprintl.com
 email: sales@iprintl.com

Advanced Data Security Features

Client 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 IPR's secure data center facilities. No inbound connections into the client's network are made during either backup or restore sessions. There is no entry attempt from a foreign source through the client firewall.

Strong Data Encryption

DataGuardian 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 IPR 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

DataGuardian 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, 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.

DeltaPro™ processing

DataGuardian uses patent pending EVault DeltaPro™ technology to speed up backup operations and drastically reduce 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. DataGuardian delivers superior performance that optimizes backup and restore functions, lowers back-end storage costs, and helps businesses gain and maintain regulatory compliance.

Optimized data compression

DataGuardian 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 DataGuardian customers, IPR'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 identify 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 protection.

Layered Security System

Based on the model being used by the Department of Homeland Security, IPR deploys a Layered Security System to protect our client's Information Assets.



Layered Security System