

OffsiteDataSync Cloud Backup Security

OffsiteDataSync employs a pioneering technology for encrypting backup data stored to disk. As information Recovery solution, encryption has been a requirement since 1995, allowing data to be securely stored and replicated to carrier-class data centers.

Data Collection

OffsiteDataSync encrypts all customer data in-flight and at-rest from cradle to grave. When collecting data from the source machines, our software establishes secure connection to any machine on the LAN using TCP/IP via existing protocols like NFS/SSH. It requires proper credentials to grab the data to be backed up from the source machines in physical or virtual environments.

Data Transport

Our technology provides extremely safe data transfer and storage using up to 256 bit encryption keys as well as all encrypted communication between all the OffsiteDataSync software. OffsiteDataSync customers can choose from encryption strengths that range from triple DES 56-bit with an 8-character key, to AES 256-bit with a 32-character key.

- DES 56-bit - up to 8-character key
- AES 128-bit - up to 16-character key
- AES 192-bit - up to 24-character key
- AES 256-bit - up to 32-character key

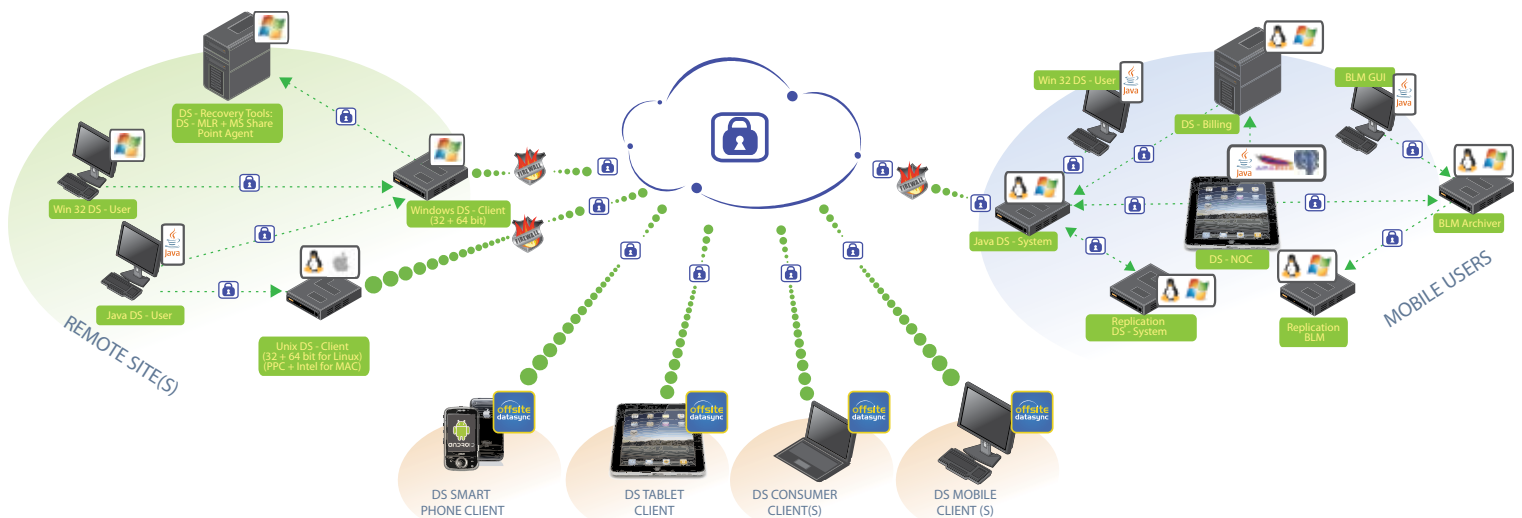
Someone monitoring data transmitted between a customer site and OffsiteDataSync Vault would intercept only encrypted data blocks. Access to confidential file content is not possible.

- Handshake between OffsiteDataSync software components
- Random encryption key for communication
- Hardware cookie registration
- IP address check for connections
- Account parameter validation

Data Storage

When the data arrives at the data center, it is stored in an encrypted format on the storage hardware. The end customer keeps the encryption keys. Hence, even a rogue employee with proper credentials inside the data center cannot access or manipulate the data. Someone who gained full access to OffsiteDataSync Vault Storage would not be able to read the contents of backed-up files, since the data is stored in encrypted format.

OffsiteDataSync Cloud Backup™ Communication Encryption for more than WAN



Encryption Key

OffsiteDataSync Cloud Backup uses two encryption keys:

1. Private key, provided by the customer at installation, used to encrypt all files except common files at the account or public level.
2. Account key, provided by the customer at installation, used to handle common files at the account level.

Encryption Security

OffsiteDataSync software stores passwords that give access to the source computers in encrypted format in its database. The OffsiteDataSync software encryption keys are also stored in encrypted format in the OffsiteDataSync software database. As a result:

1. Even a person with legitimate access to the system (such as the administrator) cannot discover the values of the encryption keys.
2. If the OffsiteDataSync software machine is compromised (a hacker gains access to this machine), the passwords that OffsiteDataSync software uses to access the source computers, and the OffsiteDataSync software encryption keys, are not compromised.

Encryption Key Safeguarding at DS-System

Encryption Key Safeguarding is an additional security provision that can be enabled from the OffsiteDataSync Vault. Forwarding the OffsiteDataSync software key(s) will send an encrypted copy of the key(s) for storage in the OffsiteDataSync Vault's database.

OffsiteDataSync cannot read customer Encryption Key(s), but will be able to create a Customer Registration Information (.CRI file) with them embedded for distribution. This means anyone who has the .CRI file can recreate a functioning OffsiteDataSync software that will be able to perform backups and restores to the corresponding account on the OffsiteDataSync Vault hardware registration may be required.

OffsiteDataSync's disk-based, automated solution runs with no human intervention. Tape backups require manual intervention and thus are not compliant with most government and industry regulations.

OffsiteDataSync employs the only data protection software that is certified and compliant with the Federal Information Processing Standards (FIPS) 140 level 2 standard. This gives government departments or regulated industries such as financial or healthcare a stamp of approval that they can use OffsiteDataSync to collect, store, and transfer their backup data.

Key Features

- All data in-flight and at-rest is encrypted
- Even a rogue employee with proper credentials cannot access or manipulate your data
- Four encryption strengths to choose from for your encryption needs: DES, AES128, AES192, AES256
- FIPS 140-2 certified
- Key escrow management
- Password rotation and management support



About OffsiteDataSync:

OffsiteDataSync delivers cloud-based data retention and disaster recovery solutions that offer effective and reliable enterprise-class data protection. OffsiteDataSync Cloud Backup and Disaster Recovery solutions are designed for IT constrained businesses and organizations with compliance mandates that remain unaddressed by traditionally unsecure, cumbersome tape-based solutions and alternate online solutions geared toward consumer-based data protection. With more than a decade of specialization in data retention OffsiteDataSync successfully protect millions of files and terabytes of data on a daily basis.