Bloombase
Least Invasive Security

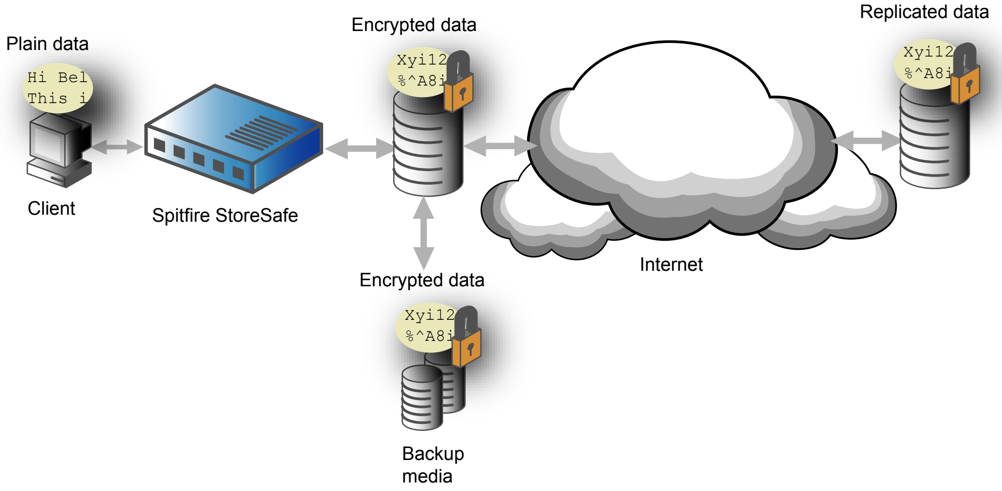
Achieving Backup and Disaster Recovery Security with Bloombase Least Invasive Security Solution

WHITE PAPER

Hardware breakdown, data center disasters and September-11 incidents raised industry's alert to maintain effective backup and disaster recovery measures to keep business running non-stop.

Mission-critical systems cannot tolerate any downtime. Computing industry developed real-time synchronization mechanism to replicate operational data from production site to disaster recovery site at near-real-time. Data replication systems do not protect replicated data on transmission. Confidential corporate information are sent as plain via the Internet exposing security concerns.

Corporate compliance and various IT governance guidelines require businesses to maintain a considerable amount of business records as archives for review in event of investigations. Business data have to be backup on separate media, sent offsite and stored in another physical location. These backup media very likely contain sensitive and secret corporate information which might get exposed to third party during transportation or in storeroom. Tape loss is one of the most frequent security threats on daily operation of enterprises with tape offsite practice.



Bloombase Solution

With Spitfire StoreSafe implemented, files are stored naturally encrypted in enterprise storage systems. Replication works directly on the encrypted data. Thus, sensitive information are sent as encrypted over the Internet. While reaching the destination, encrypted network packets are reconstructed and applied as encrypted form in replicated storage. Data replicated remain safe and secured.

Backup of corporate data is carried out directly on encrypted files without the need to go through decryption. Business data archives on backup media remain protected by strong encryption. Therefore, in worst scenario if backup tapes are lost during transportation or stolen offsite, sensitive corporate information are not going to be exposed.

Spitfire StoreSafe protects corporate and user persistence data by strong encryption. Addressing security and corporate governance compliance requirements including GLB Act, Sarbanes-Oxley Act and Personal Privacy Ordinance, etc, Spitfire StoreSafe is designed to transparently protect real-time storage data on-the-fly from unauthorized disclosure and alteration without sacrificing performance.

Spitfire StoreSafe is created to address growing security problems and paradigm shift of corporate digital data theft from company insiders since effective perimeter access control from outsiders and crackers. Internal corporate data disclosure affects company image and loss of confidential information can greatly harm enterprise goodwill and income. Spitfire StoreSafe protects data in network-attached storage (NAS), storage-area-network (SAN), tape devices and direct attached storage (DAS) supporting virtually all hardware platforms and operating systems.

Spitfire StoreSafe is a standalone storage appliance with hardware accelerated cryptographic capability to encrypt storage data as they are written to storage device and decrypt as they are read. Spitfire StoreSafe is built-in with NIST-certified secure cryptographic ciphers including FIPS-197 AES, FIPS-46-3 3DES, DES, RC2, RC4 and CAST5. Upgrade of ciphers can be done easily via a web-based user interface. Spitfire StoreSafe can run in a cluster to achieve high-availability. Spitfire StoreSafe protects databases, corporate digital assets, user files, business and financial data, archives, invaluable intellectual property, user credentials and email storage from prying eyes and tampering.

For more information, contact us at sales@bloombase.com

Bloombase
Least Invasive Security