Bloombase
Least Invasive Security

Achieving Database Protection with Bloombase Least Invasive Security Solution

WHITE PAPER

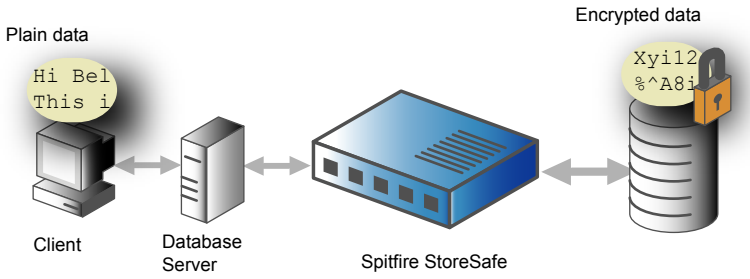
Enterprise resource and planning (ERP), sales automation, electronic marketing, financial, human resource, business intelligence (BI) and content management systems contain critical and confidential enterprise information that have to be kept secret from public access or unauthorized alteration.

Enterprise systems keep their core business data in traditional relational database management systems (RDBMS), XML databases, object-oriented databases or at least filesystems. Most if not all database management systems only protect data by access control without effective strong encryption. Anyone who can get access to database files can restore the entire database by database restoration tools or in more sophisticated cases, by scanning physical disk structure.

Secret corporate data stored in database risk theft and unauthorized alteration. However, majority of database management vendors do not have built-in database encryption capabilities. Even if they do, the encryption toolkits are over-complicated and difficult to deploy in actual environment.

Command mode encryption toolkits are mostly offered free and bundled with operating systems. However, encryption utilities can work on only offline files and the unit of work is limited to an entire file, thus, a minor update of a huge file still requires decrypt and encrypt the whole big file which is time and resource consuming. Command mode solutions are not suitable for database protection.

Partition and volume based encryption software gives way to online file encryption. However, as these solutions work on the kernel layer, solution is extremely specific to an operating system. There is not a single solution to support any platform, portability is a big issue. On the other hand, there are unforeseeable risks in compliance and support on future evolving platform upgrades.



Bloombase Solution

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

Bloombase Technologies - Least Invasive Security **email** info@bloombase.com **web** bloombase.com