BLOOMBASE®

BROCHURE

Bloombase StoreSafe

Enterprise Storage At-Rest Data Security Software Appliance

Enterprise Persistent Data at Risk

The advances in Internet, network infrastructure and technologies in the past decade opens up a new arena in network computing. What used to exist only in large enterprises' IT environment including distributed computing, network storage and electronic data exchange now become common practice in even smallest enterprises. Business data quickly develop from non-confidential historical data mainly for analysis and archival, to real-time operational data and instructions that are required to be kept secret and once presented, should never be altered. Computing infrastructure management also changed from in-house professionals to outsourced services which are broadly accepted lack of control and potentially unsafe.

This technology trend brings computing vulnerabilities in recent years from intrusion by hackers, worms and viruses, to unauthorized data alterations and data thefts, no matter physical or electronic. Data theft and unauthorized tampering greatly lower customers' confidence to a business and in most cases introduce immediate financial loss and tremendous remedial work.

The Technical Solution and the Downside

Perimeter security control measures including firewall and content filters are created to address intrusions from outsiders, however, statistics have shown that there is a paradigm shift of attacks from outsiders to insiders. To combat insiders' attack, enterprises can seek for data encryption so that in worst case scenario when data really get stolen, no one can obtain the true information from the ciphered contents.

Despite the risk of enterprise data leakage due to data theft, organizations are slow to implement data encryption.

Data encryption carried out by traditional silo-based tools are of poor performance, require complex application integration and worst of all, are difficult to scale for the most demanding business use and be extended to virtual data centers, big data and cloud applications.

Revolutionary Approach

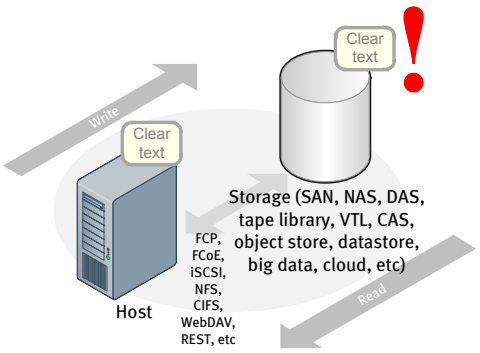
Bloombase StoreSafe delivers ground-breaking non-disruptive, application-transparent data cryptographic processing and secured centralized key management as a complete solution for enterprise-scale storage systems on both on-premises and off-premises infrastructure.

Bloombase StoreSafe is a powerful, versatile, and unified storage security software appliance to protect enterprise data without requiring drastic platform, application and user workflow change.

How It Works

Digital assets including financial reports, legal documents, private human resources information, confidential contracts and sensitive user data are invaluable properties of an organization. A business cannot risk losing these information, both confidentiality and non-repudiation have to be enforced.

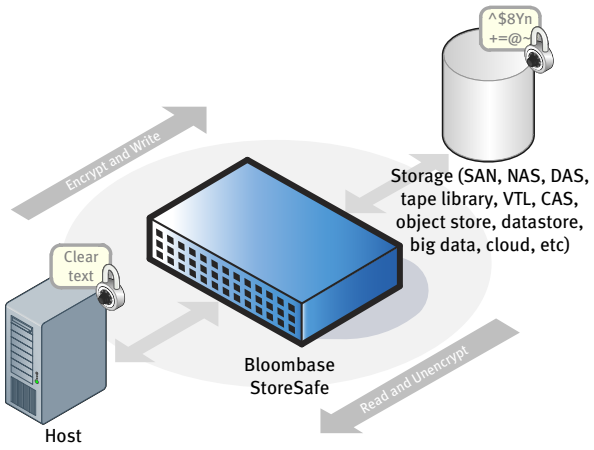
However, information created by applications are persisted in enterprise storage in plain-text. Administrators and operators can easily get direct access to the core storage system which poses potential risk of sensitive data disclosure due to data theft or attack at the storage infrastructure. Poor management of physical computing assets or offsite backup also opens up chances getting secret data exposed.



A typical storage architecture that are seen in majority of enterprises and organizations where data are persisted at storage in clear-text. Direct attack at the core readily obtains the most confidential and invaluable business and customer data.

Bloombase StoreSafe is a high performance at-rest data cryptographic server operating as a proxy to the protected storage. Bloombase StoreSafe is deployed along the path running between hosts and storages. By writing data through StoreSafe to the storage network, the encryption engine transforms plain text data into ciphered data and locks down on storage.

Trusted applications retrieving data from storage through StoreSafe gets unencrypted automatically. Bloombase StoreSafe operates as man-in-the-middle presenting the backend encrypted storage as if plain-text to host applications.



Bloombase StoreSafe operates as software appliance providing access paths for authorized hosts and applications to retrieve virtual-plain contents of protected data persisted in enterprise storage network.

Highly Secure and Manageable

Bloombase StoreSafe possesses a highly extensible cryptographic engine to cipher and decipher at-rest data on-the-fly. Bloombase StoreSafe offers rich choices of cryptographic ciphers including AES, Camellia, ARIA, 3DES, DES, CAST*, RC*, etc for data encryption.

Bloombase StoreSafe offers access control capabilities to enterprise storage systems enabling access of data in configurable volume, directory, mount point and cloud storage service endpoint. Bloombase StoreSafe works with all generic hardware and operating systems, and supports a large variety of storage protocols.

Bloombase StoreSafe is built-in with rich auditing out of the box. Administration and configuration are easily provisioned with web-based management console or via remote API. Bloombase StoreSafe supports high availability for mission-critical use and integrates seamlessly with third-party key management tools for maximum security.

Functions and Features Highlights

- Hardware and operating system independent. All physical, virtual and cloud platforms conforming to industrial storage communications protocols are supported
- File-system independent. Bloombase StoreSafe operates on storage network layer abstracting file-system underneath and above
- User independent and transparent processing. No user training required. Data stored are encrypted and data read are unencrypted automatically under the covers requiring no change on user workflow
- Transparent encryption and unencryption. High performance cryptographic engine secures storage data by strong encryption based on user-predefined rules
- Effortless and riskless deployment and implementation. No application change required. No complex system integration. No user workflow change. No administration and operation change
- Flexible and secure access control. Fine-grain network, host and user access control suiting all enterprise needs
- Multi-user support and resource sharing. Users protect their own digital assets by their own encryption keys. Resource sharing made possible without sacrificing security
- Seamless integration with Bloombase KeyCastle. Where encryption keys are required to be stored and managed separately - Bloombase StoreSafe integrates with KeyCastle seamlessly for maximum encryption key security
- High availability and clustering. Highly scalable and multiple StoreSafe instances running in a cluster for mission-critical applications and load-balancing for throughput storage systems

Business Benefits and Applications

Transparent database encryption

- Protect real-time ERP, financial and customer data in databases by on-the-fly StoreSafe storage encryption. Applications work with virtual private data without drastic performance penalty

Virtualization, big data and cloud protection

- Bloombase StoreSafe software appliance fills the missing piece for virtual datastores, analytics data nodes, and cloud storage in virtualization, big data and cloud computing infrastructure

Digital Intellectual property protection

- Design files, source codes, product prototypes and marketing campaign resources managed in file servers, CMS and DMS should be protected by strong encryption at backend storage and transparently accessible by end users and applications

Email repository encryption

- Enterprise messages contain vast amount of business secrets. Bloombase StoreSafe secures any enterprise messaging systems and groupware without requiring user workflow change

Bloombase StoreSafe configuration settings are provisioned easily by web-based management console.

Secure replication and disaster recovery

- Replication of data in their native encrypted form with cipher-text replicated in disaster recovery infrastructure. Invaluable operational data are kept privately safe and risk free

Secure data backup and archival

- Protect backup files and archives, backup tapes and disks by strong encryption to prevent leakage of secret corporate information in event of media thefts or loss

Technical Specifications Highlights

Cryptographic Security

- NIST FIPS 140-2 validated cryptographic module
- IEEE 1619 Security in Storage standards
- RSA, AES, Camellia, ARIA, 3DES, DES, CAST*, RC* cipher algorithms
- Volume-based, network share-based, file-based and object-based security
- Digital signature generation and signature verification

Access Control Security

- Fine grain read/write access control
- Host and user-based access control

Storage Networking Protocols

- FCP, FCoE, iSCSI, SCSI, NFS, CIFS, FTP, HTTP, REST
- Network and host-based authentication and authorization
- User-based authentication and authorization

Key Management

- Bloombase KeyCastle key lifecycle management
- PKCS#11 hardware security module and OASIS KMIP-compliant key manager

Management and Monitoring

- SNMP (v1, v2c, v3), syslog, log rotation and auto-archive

Administration

- SSL-secured web-based and text-mode management console
- Command line interface and API-based remote management

Bloombase - Next Generation Data Security **email** info@bloombase.com **web** www.bloombase.com

BLOOMBASE®