BLOOMBASE®

Solution Brief

Bloombase StoreSafe Data-at-Rest Encryption with IBM Security Key Lifecycle Manager

Transparent data-at-rest encryption for heterogeneous datacenter environment with simplified, centralized and automated encryption-key management

Highlights of Bloombase StoreSafe

Bloombase StoreSafe delivers turnkey, agentless, non-disruptive, application-transparent data-at-rest encryption security to lock down business sensitive information.

- Deliver encryption for on-premises disk arrays over network storage protocols including FCP, FCoE, NFS, CIFS, HTTP, WebDAV, FTP and so on
- Provide multi-tenancy encryption protection on virtual datacenter
- Secure compute instances and RESTful storage services on cloud
- Enable trusted software applications to retrieve ciphertext securely as if they were plaintext without the expensive need for application adaptation
- Mitigate outbound data threats and data leakage with low total cost of ownership (TCO)
- Immediately satisfy stringent data confidentiality and security regulatory compliance requirements
- Maximize your return on investment (ROI) on existing datacenter and storage infrastructure and avoid encryption silos
- Easily assign and manage security rules, policies and data encryption requirements
- Allow the seamless migration of sensitive data to public cloud and third-party managed datacenter environments without losing control over data privacy

IBM Registered Business Partner

Ready for Security Intelligence

Unauthorized data exposure remains a critical, yet unresolved problem, for many organizations. The causes can be both intentional (hardware theft, espionage and so on) and unintentional (media loss, viral attacks, and so on). The unbridled rate at which global businesses are taking advantage of off-premises cloud and managed services is only going to exacerbate the problem: These offerings can increase the risk of exfiltration and infiltration, regardless of the number of network defenses in place.

A paradigm shift in the approach to data management is evident: There is a movement away from managing restricted sets of critical data stored in structured relational database management systems (RDBMS), to the management and storage of virtually everything and anything. There is also a concomitant shift in the way data is stored: from on-premises storage infrastructure to off-premises cloud, platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS), managed service provider (MSP), and so on. Although the use of data encryption is vital for the protection of information, traditional database-level encryption does not work with unstructured data for analytics and big data applications. Furthermore, proprietary point-based encryption tool kits are hard to maintain and costly to integrate into existing software applications. Then, there is storage-based encryption, which involves hardware infrastructure changes and reinvestment, often resulting in vendor lock-in, posing obstacles when migrating to the cloud.

Bloombase StoreSafe is an agentless, turnkey encryption solution for data-at-rest applications. Its nondisruptive, application-transparent and protocol preserving features make it ideally suited to protecting a plethora of storage infrastructures. It secures infrastructures from on-premises storage systems [including IBM Storwize SAN, NAS, DAS, disk storage systems, tape library, virtual tape library (VTL), content addressable storage (CAS) and object stores, for instance] to virtualization (datastores of hypervisors including IBM PowerVM and KVM), big data (scale-out storage) and even off-premises cloud storage services (IBM SoftLayer/ Bluemix Object Storage, Block Storage and File Storage, OpenStack Swift and Cinder, Amazon S3, EBS and EFS, Google Cloud Storage, and Microsoft Azure Storage, for example).

Bloombase StoreSafe operates almost like a proxy over heterogeneous networked storage environments. To the network, the solution appears like a standards-based LUN, network share, backup target or even RESTful storage service endpoint. As applications make data storage requests, Bloombase StoreSafe automatically and transparently encrypts the plaintext data payload before it is physically made persistent in the storage backend as ciphertext. Likewise, decryption of ciphertext is performed “on the fly” as data is requested from the persistent storage, presenting the virtual cleartext to the requesting application as if it were never encrypted. This schema guarantees operational transparency and maximum interoperability. Unauthorized clients accessing data from a StoreSafe-secured storage will be unable to interpret any extracted data as it is already an encrypted ciphertext.

Supporting a host of industry-standard protocols, StoreSafe is application transparent, operating-system agnostic, portable across storage technologies and vendor neutral. Purpose-built, StoreSafe is a software appliance adapted for deployment on commercial-off-the-shelf (COTS) Intel or Power-based hardware servers in both physical and virtual datacenters. It can also be deployed on hypervisors and private clouds as virtual appliances, or as compute instances on cloud computing infrastructures.

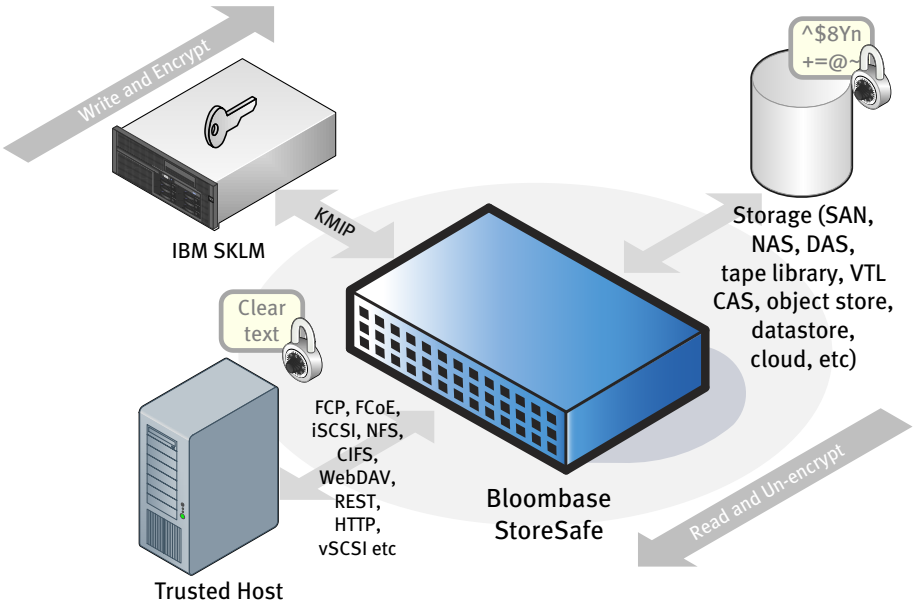
Solution Brief

IBM Security Key Lifecycle Manager

IBM Security Key Lifecycle Manager (SKLM) - formerly Tivoli Key Lifecycle Manager (TKLM) - centralizes, simplifies and automates the encryption key management process to help minimize risk and reduce operational costs of encryption key management. It offers secure and robust key storage, key serving and key lifecycle management for IBM and non-IBM storage solutions using OASIS Key Management Interoperability Protocol (KMIP).

IBM Security Key Lifecycle Manager helps customers meet regulations and standards such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and General Data Protection Regulation (GDPR) of the European Union (EU) by providing centralized control and management of encryption keys.

- Simplify, centralize and automate the encryption-key management process
- Centrally manage encryption keys to enhance data security and help facilitate regulatory compliance
- Reduce key management costs by automating the assignment and rotation of keys
- Gain flexibility with support for the encryption-key management standard - the Key Management Interoperability Protocol (KMIP) from the Organization for the Advancement of Structured Information Standards (OASIS) consortium
- Help address regulations such as PCI-DSS, which call for strong protection of encryption keys and control of the processes that manage them



Bloombase StoreSafe and IBM Security Key Lifecycle Manager: Security and Management

The Bloombase StoreSafe solution integrates with any standards-based key management tools from hardware security modules (HSM) to OASIS KMIP key managers like IBM Security Key Lifecycle Manager. StoreSafe provides high bandwidth, robust encryption of storage data and the offloads key management functions to the IBM Security Key Lifecycle Manager.

Together, IBM and Bloombase deliver a unique, transparent encryption protection of data-at-rest with centralized key management to secure operational and backup data on any datacenter infrastructure seamlessly at zero operational change.

By segregating key management and encryption duties, customers mitigate outbound data threats while meeting data privacy regulatory compliance requirements cost effectively. Because of its form factor as software and purpose built for standards-based, the solution is futureproof for next generation datacenter and storage technologies.

Highly scalable, the solution is built to secure data paths for mission-critical applications.

Customers can also centrally create, import, distribute, back up, archive and manage the lifecycle of keys by consolidating their existing key management tools.

Both Bloombase StoreSafe and IBM Security Key Lifecycle Manager products have achieved NIST FIPS 140-2 certification. For customers requiring even higher levels of tamper resistant protection of encryption keys, IBM offers the option to deploy hardware security modules (HSM) to store the master keys that are used to protect the application keys stored in the IBM Security Key Lifecycle Manager keystore.

The Bloombase StoreSafe and IBM Security Key Lifecycle Manager solution has been interoperability validated and has received the IBM Ready for Security Intelligence certification.

Learn More

For more information of IBM Security Key Lifecycle Manager, visit https://www.ibm.com/software/products/us/en/keylifecyclemanager

To learn more about Bloombase Next Generation Data Security solutions, contact your Bloombase sales representative, or visit https://www.bloombase.com

BLOOMBASE®

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

Copyright 2017 Bloombase, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Bloombase, Spitfire, Keyparc, StoreSafe, and other Bloombase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Bloombase in United States and/or other jurisdictions. All other product and service names mentioned are the trademarks of their respective companies. The information contained herein is subject to change without notice. The only warranties for Bloombase products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Bloombase shall not be liable for technical or editorial errors or omissions contained herein. Item No. BLBS-SB-Bloombase-StoreSafe-IBM-Security-Key-Lifecycle-Manager-SKLM-Data-at-Rest-Encryption-Solution-USLET-EN-Ro.96