BLOOMBASE®

BLOOMBASE STORESAFE SALES CHEAT SHEET

Overview

Bloombase StoreSafe storage security software appliance provides turnkey, non-disruptive, application-transparent encryption security of data-at-rest (DAR) from physical data center, virtual data center, big data, to the cloud.

Bloombase StoreSafe enables organizational customers to secure their structured and unstructured stored data with state-of-the-art cryptographic technologies at minimal application and infrastructure change.

Value Propositions

- Allow turnkey encryption security of data-at-rest without any changes in application, infrastructure, administrator and end-user workflow
- Provide a unified data-at-rest encryption solution to secure on-premise storage systems from unified storage, data backup and next generation storage services in both physical and virtual data centers
- Support deployment on commodity off-the-shelf (COTS) hardware appliances, as virtual appliances on virtual hypervisors and as compute instances on cloud infrastructures
- Fulfill stringent information privacy regulatory compliance requirements including PCI DSS, SOX, HIPAA, HITECH, Personal Data Privacy Law, etc, immediately and cost-effectively
- Mitigate risks and liabilities in event of data exposure
- Harden security of storage data services as last-line-of-defense from various data leakage, exfiltration, outbound and insider threats
- Eliminate vendor lock-in and end-of-life impact as with traditional hardware encryption tools
- Offer flexibility, agility, robustness and sustainability for long-term storage security needs
- Support rich set of security-proven cryptographic cipher algorithms from AES, RSA, Twofish, Blowfish, etc to various other regional cipher standards including Camellia, SEED, ARIA, SCB2, etc enabling organizations to fulfill data privacy requirements
- Provide data-at-rest encryption security as a turnkey service by eliminating complex second-development of encryption at the application-layer

Key Selling Points

How to implement data encryption without investing headcounts on code development?	■ Turnkey encryption over storage networking layer ■ No crypto API, SDK and second-development ■ Data encryption as-if moving from a disk to another ■ Zero learning curve for administrator, operator and end users
How to implement a unified encryption solution for an heterogeneous storage environment?	■ Block-based, share-based, file-based, object-based encryption in a single solution ■ Block-based encryption for FC-SAN, iSCSI, IP-SAN, etc ■ Share/file-based encryption over NFS, CIFS, HTTP, etc ■ Object-based encryption over RESTful protocols including AWS S3, EMC Atmos/ViPR, OpenStack Swift, etc ■ Sequential storage encryption for tape libraries and VTL over FCP, iSCSI, etc
How to accelerate adoption of and migration to cloud?	■ Turnkey, non-disruptive, application-transparent ■ Security proven: NIST FIPS 140-2 certified ■ Industry standard: IEEE 1619 compliant ■ Realize true separation of duty (data owner, operator, administrator) ■ Lower impact of sensitive data exposure in event of security breach and data leakage when migrated to cloud
How to avoid vendor lock-in for data encryption?	■ Encryption-as-a-service over standards-based networked storage protocols ■ Unlike silo-based, point-based, disparate encryption tools such as crypto APIs, database encryption, file-system encryption, or self-encryption drives (SED) which are vendor sticky
How to improve data access rates with encrypted databases?	■ Bloombase provides encryption on the networked storage layer regardless of structure of data being protected ■ Encryption throughput scales with number of processors allocated ■ Intel AES-NI hardware cryptographic acceleration achieves 5-10x boost in real-time encryption performance gain ■ Zero change to database schema and objects ■ No index corruption ■ Application transparent
How to meet "minority" encryption needs as a solution for global deployment?	■ Pluggable cipher architecture enabling organizations to meet global and local encryption needs as a single unified data-at-rest security solution ■ Built-in industry-standard encryption cipher algorithm support including AES, RSA, DES, 3DES, Blowfish, Twofish, etc ■ Camellia cipher support by NTT and Mitsubishi Electric for Japan ■ SEED and ARIA ciphers support for Korea ■ McEliece and qTESLA post-quantum cryptographic ciphers support ■ Kalyna cipher support for Ukraine/CIS ■ SCB2 cipher support for China
How to implement a data encryption solution that integrates seamlessly with existing key management facility?	■ Standards-based key management protocol support including OASIS KMIP and PKCS#11 ■ Bloombase-proprietary KeyCastle key management support

Competitors

Brocade/IBM/HP Encryption Switch and Blade	■ Hardware-based encryption product ■ Limited storage support on FC-SAN only ■ Not designed for virtual data center and cloud infrastructure ■ Limited cipher support on AES only
Gemalto/SafeNet StorageSecure	■ Hardware-based encryption product ■ Limited storage support on NAS only ■ Not designed for virtual data center and cloud infrastructure ■ Limited cipher support on AES only
Thales/Vormetric Transparent Encryption	■ Agent-based encryption ■ Client piece is required to be installed onto host OS and file-system ■ Limited OS support ■ Limited cipher support on AES only
CipherCloud	■ SaaS encryption for hosted applications including Gmail and Salesforce only ■ Not designed for generic data center platform and on-premise IT infrastructure

Qualifying Questions

Is customer one of Global 500 scale organizations?	Fortune Global 500 scale multi-national corporations manage vast amount of business sensitive data in complex heterogeneous IT environment that needs protection
Are you from market verticals in which data privacy regulatory compliance is mandatory?	Bloombase provides turnkey data-at-rest encryption security of stored data enabling organizations to meet data regulatory compliance easily and cost-effectively. Organizations from segments including banking and FSI, public, healthcare and medical manage large volume of end customer information requiring encryption
Are you from market verticals which deal with a lot of intellectual properties, business know-hows and trade-secrets in your day-to-day operations?	Bloombase delivers non-disruptive protection of your invaluable digital assets from leakage and exfiltration threats. Data can be locked down on storage systems and services, enabling data owners to retrieve these business sensitive information as-if they are in the clear without workflow change. This achieves separation-of-duties allowing administrators and operators to manage the IT infrastructure without being able to access the business sensitive digital assets. Organizations from oil-and-gas, technology, chemical and pharmaceutical, research, defense and aerospace are well qualified as Bloombase customers
Are you challenged by the need for data encryption with complex heterogeneous business applications, host operating systems and storage infrastructure?	Bloombase provides a unified, platform-neutral, application-transparent encryption of data-at-rest over networked storage layer
Are you moving application workload and data to cloud infrastructure managed by MSPs?	The level and scale of exposure by migrating on-premises data to off-premises cloud managed by outsourced service providers are much higher. Off-premise business sensitive data deserves proper protection
Is your storage infrastructure built with high-end storage systems and services?	Chances sensitivity of stored data higher for organizations running high-end storage systems and services
Any existing data-at-rest encryption tools running in your IT environment?	Customers running NetApp/Decru DataFort, Thales/nCipher/NeoScale CryptoStor, CipherMax/MaXXan, Gemalto/SafeNet/Ingrian DataSecure, Protegrity, Sophos/Utimaco SafeGuard LAN Crypt, etc are challenged by product end-of-life (EOL) and service end-of-support (EOS) with immediate need for rescue and product replacement

Objection Handling

Customer already has encryption	Customers can sometimes get confused with data-in-flight and data-at-rest. When they specifically say they already have encryption, check if they are referring to HTTPS, SSL, TLS, IPsec, link encryption, etc which are just data in-flight/in-motion encryption only. Some customers may truly have encryption of at-rest data implemented but simply at the application or database layer which is risky to implement and costly to maintain. The fact that application and database data are mainly structured-data, however, the expansion of enterprise data is largely unstructured and located in heterogeneous data center environment and storage infrastructure accessed by heterogeneous storage networking protocols. To deal with the challenging growth of these data driven by big data, analytics and likely Internet of Things and Internet of Everything, in which sensitive information are all over the place, customers need a unified, turnkey easy to manage, easy to implement encryption solution which is able to scale from physical, virtual data center to cloud and being able to be future-proof.
End-point security products have built-in data-loss-protection (DLP) support	Data loss protection (DLP) tools protect data privacy from leakage in event of portable/mobile hardware/media loss only. It is not designed to secure long term retention of storage data in data center infrastructure and does not provide enterprise-grade full life-cycle key management support.
Customer already has key management tool and hardware security module (HSM)	Key management tools (e.g. OASIS KMIP, PKCS#11, etc) mainly deal with life-cycle management of encryption keys whereas hardware security modules (HSM) provide tamper-proof and tamper-resistant key storage and protection for higher standard of key security. Customers having deployed key management tools and HSMs only get part of their data protection problem solved which is merely key management. When it comes to actual encryption of their business critical data, they are required to implement separate encryption in their business applications by integrating with these key tools. Often times this traditional process from data classification, application second development, testing, tuning, to migration takes more than 6 months whereas for Bloombase approach, in a week's time.
Database encryption is already in place	Database encryption tools are costly to maintain, sticky on specific database vendor and version, and oftentimes of low efficiency. Bloombase to serve as customer option with capability to secure database files and volumes on storage networking layer as a more future-proof and efficient solution.
Perimeter security measures are already adequate	Cyber-attacks from the outside can effectively be blocked by network security tools including intelligent firewall and content filters. Storage encryption solutions such as Bloombase helps mitigate the worsening threat of data exfiltration problem caused by insiders.
Data encryption would significantly slow down software applications	Traditional database encryption and file-system encryption are inefficient by competing for computing resources with business application workload. Bloombase provides next-generation stored data encryption as a separate piece and allows scale-up and scale-out flexibly.
Encryption could cause data corruption	Standards-based cryptographic algorithms are proven and have been utilized extensively to secure e-commerce applications. Bloombase supports various robust industry standard encryption cipher algorithms to secure mission critical application data. To avoid potential data loss and facilitate data restoration/recovery, customers should practice effective backup of ciphertext stored data along with the encryption key(s) securing the data.
Encryption is costly to deployment and maintain	Bloombase software products offer flexible licensing model which adapt to any scale of deployment. The software appliance can be deployed on cost effective COTS hardware appliance to deliver encryption services.
No urgency with encryption: no data classification and no definite data protection guidelines	Customers should take prompt action to secure their business sensitive data otherwise they might risk security breaches and data leakage which could lead to adverse effects to their business operations and company goodwill

Performance Benchmark (Per Processor-core / vCPU)

FCP	2 Gbps *
iSCSI	1 Gbps *
NFS	0.5 Gbps *
SMB/CIFS	0.4 Gbps *
REST/HTTP	0.25 Gbps *

* with Intel AES-NI

MSRP

Processor-core Perpetual License	US$16,800.00 †
Processor-core 1-Year Term License	US$3,360.00 †
Processor-core 2-Year Term License	US$5,880.00 †
Processor-core 3-Year Term License	US$8,400.00 †
Processor-core 4-Year Term License	US$10,080.00 †
Processor-core 5-Year Term License	US$11,760.00 †
1-Year Basic Technical Support	US$2,688.00 †
1-Year Premium Technical Support	US$3,528.00 †
3-Year Basic Technical Support	US$8,064.00 †
3-Year Premium Technical Support	US$10,584.00 †

† as of FY20 Q1

Package Offer by Example

1-node 1-way quad-core x86-processor single-node setup with first year premium technical support (max 8Gbps encryption throughput)	1 * 1 * 4 * 0.5 * US$16,800 * 1.21 = US$40,656.00 ‡
1-node 1-way quad-core x86-processor HA cluster setup with first year premium technical support (max 8Gbps encryption throughput)	1 * 2 * 4 * 0.5 * US$16,800 * 1.21 = US$81,312.00 ‡
2-node 2-way quad-core x86 processor HA cluster setup with first year premium technical support (max 16Gbps encryption throughput)	2 * 2 * 4 * 0.5 * US$16,800 * 1.21 = US$162,624.00 ‡
2-node 2-way eight-core x86 processor HA cluster setup with first year premium technical support (max 32Gbps encryption throughput)	2 * 2 * 8 * 0.5 * US$16,800 * 1.21 = US$325,248.00 ‡
2-node 4-way eight-core x86 processor HA cluster setup with first year premium technical support (max 64Gbps encryption throughput)	2 * 4 * 8 * 0.5 * US$16,800 * 1.21 = US$650,496.00 ‡
2-node 4-way sixteen-core x86 processor HA cluster setup with first year premium technical support (max 128Gbps encryption throughput)	2 * 4 * 16 * 0.5 * US$16,800 * 1.21 = US$1,300,992.00 ‡

‡ as of FY20 Q1

Engagement Model

To engage Bloombase in business opportunity, reach out to our Global Sales Operations team at email gso@bloombase.com directly, we will identify the product specialist(s) to support you and your customers.

The sales process would include lead qualification, product evaluation, solution proposition, sizing, etc.

For further information, please visit https://www.bloombase.com/go/productinfo.

For deal registration, please visit https://supportal.bloombase.com/supportal/submit_lead.jsp.

To request for a product evaluation kit, please visit https://www.bloombase.com/go/evalkit.

Additional Information

Bloombase StoreSafe product brochure	https://www.bloombase.com/content/9082VHud
Bloombase StoreSafe technical specifications	https://www.bloombase.com/content/8936QA88
Bloombase StoreSafe compatibility matrix	https://www.bloombase.com/content/8396639C
Bloombase / AWS solution brief	https://www.bloombase.com/content/fVjOxbwc
Bloombase / Dell solution brief	https://www.bloombase.com/content/UYpUsgZQ
Bloombase / EMC solution brief	https://www.bloombase.com/content/W9pfThdR
Bloombase / HDS solution brief	https://www.bloombase.com/content/DsRDs8xi
Bloombase / IBM SKLM solution brief	https://www.bloombase.com/content/txuaKvBs
Bloombase / Intel solution brief	https://www.bloombase.com/content/iqqEIrAU
Bloombase / KVM solution brief	https://www.bloombase.com/content/fBwXRRf5
Bloombase / Micro Focus ESKM solution brief	https://www.bloombase.com/content/dEjXPo5z
Bloombase / Microsoft solution brief	https://www.bloombase.com/content/L7bEST1J
Bloombase / nCipher solution brief	https://www.bloombase.com/content/jKlxcGwU
Bloombase / Thales solution brief	https://www.bloombase.com/content/GzIRSH7E
Bloombase / VMware solution brief	https://www.bloombase.com/content/5WLHL7rP

BLOOMBASE®

Bloombase - Intelligent Storage Firewall **email** info@bloombase.com **web** https://www.bloombase.com