

Bloombase StoreSafe Security Server



Features

Application Transparent Data-at-Rest Security with Storage Virtualization

High performance and intelligent storage virtualization technology delivers security processing of data-at-rest based on data-owner-defined security rules and policies. No user training is required. Data protected is secured on-the-fly requiring no change on user workflow and application logic.

Hardware, Platform and Filesystem Independent

Bloombase StoreSafe supports all platforms conforming to standards-based storage networking protocols and it operates on the storage networking layer abstracting filesystem underneath and software applications above.

High Performance

Leveraging Intel AES-NI and various other third-party hardware cryptographic acceleration technologies to minimize performance degradation as a result of latency with real-time encryption and decryption, pushing encryption speed to the limits meeting throughput-computing needs.

Flexible and Secure Access Control

Fine grain user and host access control suiting all enterprise storage security needs.

High Availability

Highly scalable and multiple Bloombase StoreSafe software appliances running in cluster for failover in mission-critical systems and load-balancing for high-throughput storage applications.

Security

NIST FIPS 197 AES cipher algorithm support (NIST certificate #1041)

IEEE 1619-compliant AES XTS block cipher

RSA public key cryptography (NIST certificate #496)

SHA-1, SHA-256, SHA-384, SHA-512 hash generation (NIST certificate #991)

Accredited keyed-hash message authentication code generation (NIST certificate #583)

Japan NTT/Mitsubishi Electric Camellia cipher algorithm support

Korean SEED and ARIA cipher algorithm support

GOST, Kalyna and SM4 cipher algorithm support

NIST FIPS-46-3 3DES and DES cipher algorithm support

RC2, RC4, RC5 and RC6 cipher algorithm support

CAST5 cipher algorithm support

Twofish and Blowfish cipher algorithm support

IDEA cipher algorithm support

Serpent and Skipjack cipher algorithm support

Pluggable cipher architecture for future cipher upgrade or custom cipher support

Obfuscation and data shuffling for simple data hiding

Storage Systems

Direct Attached Storage (DAS)

Network Attached Storage (NAS)

Storage Area Network (SAN)

Tape library, tape drive and virtual tape library (VTL)

Content Addressable Storage (CAS) / Cloud Storage / Object Store

Privacy Control

Automated file-based and block-based encryption on storage device and file write operations

Automated decryption on storage device and file read operations on trusted hosts and clients

Multiple key encryption

Fix-sized file header regardless of actual file size for file-based protection

No additional storage required for block-based protection

Access Control

Fine grain read/write/create/delete/list access control

Time-window-based access control

Zero alteration to actual storage contents

Zero impact to performance

Integrity Control

Automated filesystem object digital signature generation

File integrity verification

Multiple key digital signature generation

Fix-sized file header regardless of actual file size

Write-Once-Read-Many (WORM)

Write-once-read-many feature resembling non-rewritable optical media supporting secure archival of data eliminating potential risks being overwritten by intention or accidental operation

For storage archival, compliance, dynamic capacity management and information lifecycle management (ILM)

Policy based engine dynamically adapts to changing demands in data requirements, by moving files automatically and transparently to appropriate tiered storage

Rule based configuration for permanently delete and/or shred file contents

Authentication and Authorization

User-based and role-based authentication and authorization

Generic Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory (MSAD) authentication and authorization

Host-based authentication and authorization

Microsoft NT Lan Manager (NTLM) authentication

Challenge Handshake Authentication Protocol (CHAP) based discovery and authentication

Direct Attached Storage (DAS)

Extensive Storage Communication Protocol Support

Fiber Channel Protocol (FCP)

Fiber Channel over Ethernet (FCoE)

Internet Small Computer System Interface (iSCSI)

Small Computer System Interface (SCSI)

Serial Attached SCSI (SAS)

Serial Advanced Technology Attachment (SATA)

Parallel Advanced Technology Attachment (PATA)/Integrated Drive Electronics (IDE), etc

Platform Independent

Bloombase OS

HP-UX

OpenVMS

IBM-AIX

Sun Solaris

Linux

Microsoft Windows

Mac OS, etc

Hardware Interoperability

HP

IBM

Sun StorageTek

Dell

HDS

EMC

NetApp

Apple

Ultra 160 SCSI low voltage differential (LVD) compliant host bus adapter (HBA)

Emulex

QLogic, etc

Filesystem Independent

Raw

ext2 and ext3

FAT

FAT-32

NTFS

UFS

ZFS

CFS

VxFS

HDFS, etc

Network Attached Storage (NAS)

Extensive Storage Communication Protocol Support

Network File System (NFS)
Common Internet File System (CIFS)
Server Message Block (SMB)
Web-based Distributed Authoring and Versioning (WebDAV)
Andrew File System (AFS)
NetWare Core Protocol (NCP)
Hypertext Transfer Protocol (HTTP)
File Transfer Protocol (FTP), etc

Platform Independent

Bloombase OS
HP-UX
OpenVMS
IBM-AIX
Sun Solaris
Linux
Microsoft Windows
Mac OS, etc

Hardware Interoperability

HP
IBM
Sun StorageTek
Dell
HDS
EMC
NetApp
Apple
Generic and TCP/IP offloading network interface card (NIC)
Neterion
Intel, etc

Filesystem Independent

ext2 and ext3
FAT
FAT-32
NTFS
UFS
ZFS
CFS
VxFS
HDFS, etc

Storage Area Network (SAN)

Extensive Storage Communication Protocol Support

Fiber Channel Protocol (FCP)

Fiber Channel over Ethernet (FCoE)

Internet Small Computer System Interface (iSCSI), etc

Platform Independent

Bloombase OS

HP-UX

OpenVMS

IBM-AIX

Sun Solaris

Linux

Microsoft Windows

Mac OS, etc

Hardware Interoperability

HP

IBM

Sun StorageTek

Dell

HDS

EMC

NetApp

Apple

Brocade

Cisco

Emulex

QLogic

ATTO Technology

Alacritech, etc

Filesystem Independent

Raw

ext2 and ext3

FAT

FAT-32

NTFS

UFS

ZFS

CFS

VxFS

HDFS, etc

Tape Library, Tape Drive and Virtual Tape Library (VTL)

Extensive Tape Communication Protocol Support

Fiber Channel

Small Computer System Interface (SCSI)

Serial Attached SCSI (SAS)

Internet Small Computer System Interface (iSCSI), etc

Platform Independent

Bloombase OS

HP-UX

OpenVMS

IBM-AIX

Sun Solaris

Linux

Microsoft Windows

Mac OS, etc

Hardware Interoperability

HP

IBM

Oracle Sun StorageTek

Dell

HDS

EMC

NetApp

Apple

Brocade

Cisco

Quantum

CommVault

FalconStor

Spectra Logic

Alacritech, etc

Content Addressable Storage (CAS) / Cloud Storage / Object Store

Interoperability

RESTful Object Store

EMC Centera

EMC ATMOS / ViPR / Elastic Cloud Storage (ECS)

Caringo CAStor and Dell Object Storage

NetApp SnapLock

Hitachi Content Platform (HCP)

Amazon Web Services (AWS) Simple Storage Service (S3), Elastic Block Storage (EBS) and Elastic File System (EFS)

OpenStack Swift Object Storage and Cinder Block Storage

Application Programming Interface

REST, Web Services, Java RMI, and C application programming interface (API)

Key Generation

NIST FIPS accredited random number generator (NIST certificate #591)

Intel Digital Random Number Generator (DRNG)

ID Quantique Quantis true random number generator support (optional)

Key Management

Multiple certificate authority (CA) support

Hardware true random (optional) or software pseudo-random key generation, inquiry and deletion

X.509 and PKCS#12 DER and PEM key import and export

Key Usage Profiling

RDBMS and Generic LDAP Support and Integration

Automatic Certificate Retrieval from Certificate Authority via HTTP or LDAP

Certificate Validity Check

Certificate Revocation Check via HTTP or LDAP

Certificate Revocation List (CRL)

Certificate Revocation List Distribution Point (CRLDP)

Online Certificate Status Protocol (OCSP)

Hardware Security Module / Key Manager Support

Amazon CloudHSM

Amazon Key Management Service (KMS)

Cavium LiquidSecurity HSM / NITROX XL

Gemalto SafeNet KeySecure

Gemalto SafeNet Network HSM / Luna SA

Gemalto SafeNet ProtectServer

Google Key Management Service (KMS)

IBM Cloud Key Protect

IBM Security Key Lifecycle Manager (SKLM) (formerly Tivoli Key Lifecycle Manager TKLM)

Microsoft Azure Key Vault

Micro Focus Atalla Enterprise Secure Key Manager (ESKM)

Oracle Sun Crypto Accelerator

Thales keyAuthority

Thales nShield

Thales payShield

Thales Vormetric Data Security Manager (DSM)

Ultra Electronics AEP Keyper

Utimaco CryptoServer / SecurityServer

PKCS#11 compliant hardware security modules

OASIS KMIP compliant key managers

Hardware Cryptographic Acceleration Support

UltraSPARC cryptographic accelerator

Intel Advanced Encryption Standard New Instructions (AES-NI)

Exar/Hifn Express DS cards

Standard Support and Certification

IEEE 1619 standard-based mode

NIST FIPS 140-2 validated Bloombase Cryptographic Module

OASIS Key Management Interoperability Protocol (KMIP) support (optional)

Management

Web based management console

Central administration and configuration

User security

Serial console

SNMP v1, v2c, v3

syslog, auto log rotation and auto archive

Heartbeat and keep alive

High Availability

High-availability option for active-active or active-standby operation

Stateless active-standby failover

Interoperable with Bloombase Quorum Server to avoid split-brain scenarios (optional)

Disaster Recovery

Configurations backup and restore

FIPS-140 hardware security module recovery key or software recovery key vault for settings restoration (optional)

Customer-defined recovery quorum (e.g. 2 of 5)

FIPS-140 hardware security module operator key or operator pin for day-to-day Bloombase KeyCastle operation (optional)

Operating System Support

Bloombase OS

Solaris

HP-UX

OpenVMS

IBM AIX

Linux

Microsoft Windows

Mac OS X



Bloombase - Next Generation Data Security

email info@bloombase.com
web <http://www.bloombase.com>

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, Inc. in United States, Canada, European Union and in several other countries all over the world. 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.

Copyright 2018 Bloombase, Inc. All rights reserved.

Specification Sheet
H87998

Virtual Platform Support

VMware vSphere / ESX / ESXi
VMware Server
VMware Workstation
Red Hat KVM
Citrix XenServer
Microsoft Hyper-V
IBM PowerVM
Oracle VM Server
Oracle VirtualBox
OpenStack

Cloud Platform Support

Amazon Web Services (AWS)
IBM Cloud / Bluemix / SoftLayer
Google Cloud Platform (GCP)
Microsoft Azure
Rackspace
Oracle Cloud

Hardware Support

i386-base architecture
AMD 32 and 64 architecture
Intel Itanium-2 architecture
IBM Power6 architecture
PA-RISC architecture
UltraSPARC architecture

Applications

ERP, CRM, RDBMS
BI, data warehouse, data mining, Hadoop, Big Data analytics
File service, CMS, DMS
Messaging, group ware, collaborations
Virtual server computing, VDI

System Requirements

System free memory space 1GB
Free storage space 2GB

Warranty and Maintenance

Software maintenance and support services are available.