Specification Sheet

BLOOMBASE®

Bloombase StoreSafe Security Server

Features

Transparent Encryption and Un-encryption

High performance and intelligent cryptographic engine sensing network storage information and carry out cryptographic operations based on user-predefined rules. No user training required. Data to be stored are encrypted and data to be read are decrypted automatically on the fly under the covers requiring no change on user workflow and application logic.

Hardware, Platform and Filesystem Independent

Bloombase StoreSafe Security Server supports all platforms conforming to industrial storage communications protocols and it operates on the storage networking layer abstracting filesystem underneath or above.

High Performance

Patent pending Bloombase Transparent Cache minimizes performance degradation as a result of real-time encryption and decryption, pushing encryption throughput to the limits at gigabit and 10-gigabit wire-speeds.

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 systems.

Security

NIST FIPS 197 AES encryption and decryption (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 encryption and decryption

Korean SEED and ARIA encryption and decryption

Chinese National SCB2(SM1), SSF33, SSF28 encryption and decryption

NIST FIPS-46-3 3DES and DES encryption and decryption

RC2, RC4, RC5 and RC6 encryption and decryption

CAST5 encryption and decryption

Twofish and Blowfish encryption and decryption

IDEA encryption and decryption

Serpent and Skipjack encryption and decryption

Pluggable cipher architecture for future cipher upgrade or custom cipher support

MD5 and Chinese National SCH(SM3) hash generation

Hardware ASIC cryptographic acceleration (optional)

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 SpitfireOS

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 SpitfireOS

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 SpitfireOS

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 SCSCI (SAS)

Internet Small Computer System Interface (iSCSI), etc

Platform Independent

Bloombase SpitfireOS

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

Caringo CAStor and Dell Object Storage

NetApp SnapLock

Hitachi Content Platform (HCP)

Amazon Web Services (AWS) Simple Storage Service (S3) and Elastic Block Storage (EBS)

OpenStack Swift Object Storage and Cinder Block Storage

Application Programming Interface

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

SSL protection

Integrate with application servers for application-level data security supporting Java, C, PHP, etc

Integrate with database servers as stored procedures for fine granular row-based and column-based data security and achieve transparent processing by database triggers supporting major databases including Oracle, IBM DB2, Microsoft SQL Server, Sybase, etc

Integrate with web browser scripting technologies for thin-client data security supporting JavaScript , etc

Integrate with OS commands and scripting tools for batch data processing supporting UNIX-like and Microsoft Windows, etc

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

Industry Standard PKCS#11 Hardware Security Module support (optional)

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 Protocal (OCSP)

Hardware Security Module Support

AEP Networks Keyper

Oracle Sun Crypto Accelerator

Sophos Utimaco SafeGuard CryptoServer

Thales nShield

HP Atalla

IBM 4758 Cryptographic CoProcessor

IBM eServer Cryptographic Accelerator

IBM Crypto Express2

IBM CP Assist for Cryptographic Function

Cavium NITROX XL

Other PKCS#11 compliant hardware security modules

Hardware Cryptographic Acceleration Support

UltraSPARC cryptographic accelerator

Intel 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 Spitfire 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

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

FIPS-140 hardware security module operator key or operator pin for daily Spitfire KeyCastle operation

Operating System Support

Bloombase SpitfireOS

Solaris

HP-UX

OpenVMS

IBM AIX

Linux

Microsoft Windows

Mac OS X

Virtual Platform Support

VMware ESX/ESXi

VMware Server

Red Hat KVM

Citrix XenServer

Microsoft Hyper-V

IBM PowerVM

Oracle VirtualBox

OpenStack

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

VDI

System Requirements

System free memory 1GB

Free storage space 2GB

Warranty and Maintenance

Software maintenance and support services are available.

BLOOMBASE®

Bloombase - Next Generation Data Security

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

Specification Sheet
H87998