CUSTOMER SPOTLIGHT

A Public Order Enforcement Government Agency in Asia

Bloombase® StoreSafe™
Storage Security Server

Bloombase® KeyCastle™
Key Management Server

Bloombase® High Availability Module

Bloombase helps an Asian law enforcement government agency accelerate highly secure electronic knowledge management, data archiving and disaster recovery and improve operational efficiency and data privacy.

AT A GLANCE

ABOUT THE CUSTOMER

- A law enforcement and special duty government organization in Asia-Pacific
- More than 30,000 users

SUMMARY

To protect operational database and backup archives of a highly regulated equipment inventory stored at EMC VNX/VNXe/Celerra to immediately comply to various information privacy regulatory standards with zero change to applications and platform

KEY CHALLENGES

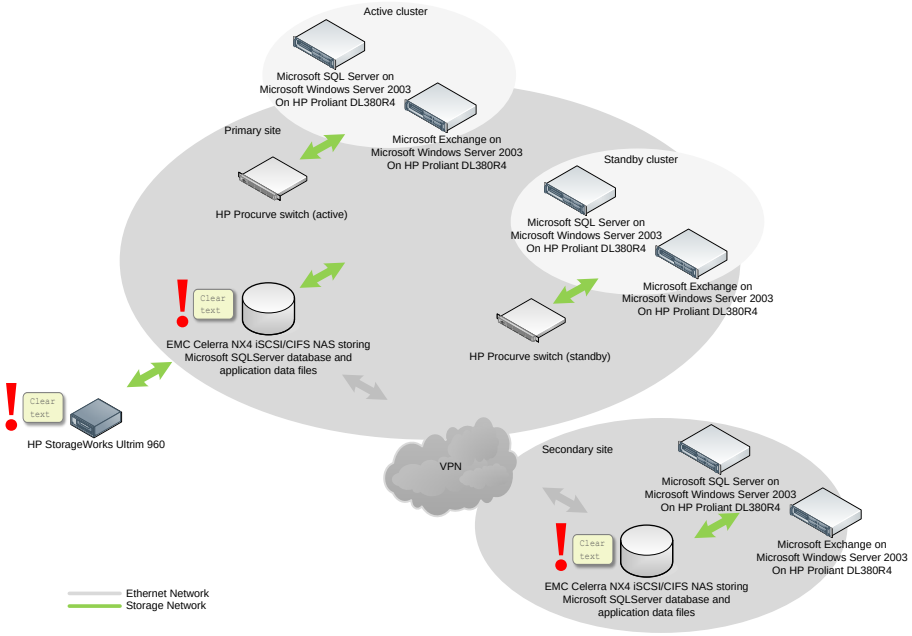
- End customer has limited budget on data encryption
- For management and daily operations concern, file-based encryption instead of volume-based is a must
- Online on-the-fly encryption and un-encryption of database without the need to change database schema
- Able to fit transparently to the in-house developed content management system (CMS) at absolutely no change to application logic
- Backup archives have to be protected from unauthorized disclosure in worst case scenario of theft or media loss
- No significant latency penalty on database, file server and data archive
- Zero change to end user, administrator and operator workflow
- No degradation to mission-critical service level agreement (SLA)
- Interoperable with future potential system changes in operating system and server hardware platform
- Key rotation without requiring intervention of database administrators and application developers

OVERVIEW

An Asian government organization responsible for enforcing civic responsibilities and countering illegal acts, manages an inventory of regulated equipment by use of a highly confidential computing system. With more than 30,000 users in the region, authorized users of the inventory system can inquire equipment particulars, manage stock levels, and retrieve intelligence reports. A special duty unit of the agency is responsible for operating physical inventory and detailed logistics in a number of controlled locations. As part of a decoupled and decentralized business operational system, the inventory runs an active cluster of system in a primary location and a backup system in a disaster recovery (DR) site, linked up by a physical private network running dedicated dark fibers.

As inventory continued to expand with more items and bigger sized multi-media objects, the system has experienced an explosion of data, amounting to over 8 terabytes (TB) currently. These data were highly unstructured managed in EMC VNX/VNXe/Celerra Unified Storage System as discrete file objects and Microsoft SQL Server tablespace files. Adding Microsoft Exchange Servers for interchange of equipment multi-media information via emails, storage data contain vast amount of sensitive information that are classified confidential and some, secret. The inventory system becomes so mission critical to the operations of the agency that its information have to be available around the clock. A disaster recovery system had to be setup to enable fast failover of services for business continuation in event of attack or service unavailability at the primary site. To comply with both data privacy and protection standards, a data at-rest security solution is needed that can transparently drop-in to the existing system, minimize impact to overall system performance, and enable true delegation of data center operations to workers and contractors.

BLOOMBASE®



BLOOMBASE SOLUTIONS

After a 3-month rigorous evaluation, end customer chose Bloombase data at-rest security protection solutions instead of volume-based or column-based encryption in early 2009 to integrate with their existing EMC VNX/VNXe/Celerra NX4 Unified Storage System and HP ProLiant Intel-based servers.

Two Bloombase StoreSafe Storage Security Server units were deployed and configured in high availability mode to serve as data at-rest encryption hub for EMC VNX/VNXe/Celerra file server at primary site. Two Bloombase KeyCastle Key Life-Cycle Management Server units were deployed as a cluster in the same facility providing key protection and storage at NIST FIPS 140-2 level 3 security. Disaster recovery site is designed without high availability in concern, therefore, Bloombase facility is simplified to single StoreSafe for real-time storage encryption and single KeyCastle for key management.

The Bloombase data at-rest encryption solution offers transparent wire-speed on-the-fly encryption and un-encryption of storage data in EMC VNX/VNXe/Celerra network storage system (NAS) requiring virtually no change in application tier. It has to provide the scalability to secure the rapidly expanding EMC Celerra storage box which accommodated 8TB of data initially to more than 16TB in 4 years' time.

ACCELERATE KNOWLEDGE MANAGEMENT AND EFFICIENCY

With Bloombase solutions, staff from different physical locations, be it a specialist capturing equipment particulars at their headquarters office, a warehouse keeper at an inventory site, or a senior official responsible for sending instructions on distribution of goods, are able to access real-time inventory information and collaboration seamlessly with each other via a web-based graphical user interface (GUI) by interacting with an application service developed in-house deployed on Windows Server 2003. Sensitive inventory information are stored at cipher-text securely stored in EMC VNX/VNXe/Celerra. The encryption and un-encryption processes are automated by Bloombase StoreSafe Security Server cluster providing virtual plain contents to authorized users and applications at full transparency.

Staff productivity in particular is greatly enhanced as officials are no longer required to spend hours or even days cross-referencing spreadsheets and documents scattered in file servers in different locations. They simply upload and download security classified information managed by Microsoft SQL Server protected by Bloombase StoreSafe anytime, whenever and wherever they need to. Imagine their old workflow by use of primitive file encryption utility, right-click-encrypt-and-check-in, check-out-right-click-and-decrypt, this so-called "secure" document management workflow is so cumbersome and hard to guarantee repetitiveness, eventually proved to be disastrous failure with all users simply checking in highly sensitive documents in plain. Thanks to Bloombase data at-rest solution, it enables application users to interact with secure documents friendly and efficiently at no addition of meaningless security workflows.

ASSURE SECURITY AND COMPLIANCE

Bloombase data at-rest solution offers advanced security capabilities for a reliable application transparent cipher-text information storage infrastructure. Its tamper-proof hardware encryption key security module ensures confidentiality and integrity throughout its whole lifecycle. Bloombase Cryptographic Module is NIST FIPS 140-2 certified providing FIPS approved RSA and AES cryptographic algorithms, together with non-FIPS ciphers including Camellia, 3DES, Twofish, Blowfish, etc.

EMC VNX/VNXe/Celerra storage targets are accessed by both iSCSI and CIFS storage protocols via Bloombase StoreSafe Security Servers. Ciphered sensitive information is stored in EMC VNX/VNXe/Celerra storage system for centralized management enabling only authorized access of virtual-plain information by trusted applications and systems per access rules and security profiles governed by Bloombase StoreSafe encryptors. Microsoft SQL Server data files, Microsoft Exchange email repository and selected file system folders and directories are protected by AES 256-bit cipher algorithm offered by Bloombase

PROJECT OBJECTIVES

- Ensures privacy of highly confidential operational data files stored at EMC Celerra storage sub-system
- Protects secrecy of databases storing sensitive inventory information of highly regulated equipment
- Encrypts sensitive data managed by an in-house developed web-based content management system (CMS)
- Secures confidential information in Microsoft Exchange email repository
- Protects storage backup archives from unauthorized information exposure
- Encryption key protection has to be at least NIST FIPS 140-2 level 3 certified
- Manages encryption keys and simplifies yearly and quarterly key rotation procedures

SOLUTIONS AND SERVICES

- Bloombase StoreSafe™ Storage Security Server
- Bloombase KeyCastle™ Key Management Server
- Bloombase High Availability Module

WHY BLOOMBASE SOLUTIONS

- Wire-speed automated encryption and un-encryption
- Able to offer data at-rest encryption at file level instead of volume level
- Offers Network File-System (NFS), Windows share (CIFS) and iSCSI virtual encryption targets with the same box
- Easily scale-up and scale-out on file servers working with
- Fulfills stringent security requirement mandating physical separation of application server, data encryption appliance and key storage appliance
- Integrates seamlessly with PKCS#11 hardware security module (HSM)
- Proven and high availability ready
- Hardware, platform and software interoperability and portability
- IEEE 1619 storage security standard compliant
- Transparent operation and administration
- True segregation of data ownership and system operation

IMPLEMENTATION HIGHLIGHTS

A highly flexible, secure, capable and adaptive data at-rest encryption solution that integrates seamlessly at both application host and storage ends

KEY BENEFITS

- Immediate compliance to stringent information confidentiality regulatory requirements
- Fast deployment and migration
- iSCSI block-based and CIFS file-based encryption in a single solution
- Highly secure NIST FIPS 140-2 level 3 total key management
- Highly available and fault-tolerant
- Wirespeed encryption performance
- Low total cost of ownership (TCO)

HARDWARE

- HP ProLiant DL380R4 server
- HP ProCurve switch
- EMC VNX/VNXe/Celerra NX4 storage sub-system
- HP StorageWorks Ultrium 960 tape library
- Sun Microsystems Sun Fire X4150 server
- Sun Crypto Accelerator 6000 hardware security module (HSM)

OPERATING SYSTEM

- Microsoft Windows Server 2003
- Microsoft Windows XP

SOFTWARE

- Microsoft SQL Server
- Microsoft Exchange Server
- Symantec Veritas Backup Exec
- Symantec Antivirus

StoreSafe virtual storages, enabling application servers to achieve various information privacy compliance standards immediately and effectively.

EASE OF MANAGEMENT AND RELIABLE SECURITY

The easy-to-manage Bloombase security solutions help end customer enforce data confidentiality for storage, which improves overall system security, enables fast key rotation, reduces user workflows, segregates data ownership from administration and operation, and enhances efficiency and internal controls.

Leveraging on its Bloombase information security infrastructure, end customer has also successfully migrated its archival system from plain data backup to one with born-to-have encryption. End customer is able to enjoy high-speed secure data backup without affecting the server cycles or backup process times.

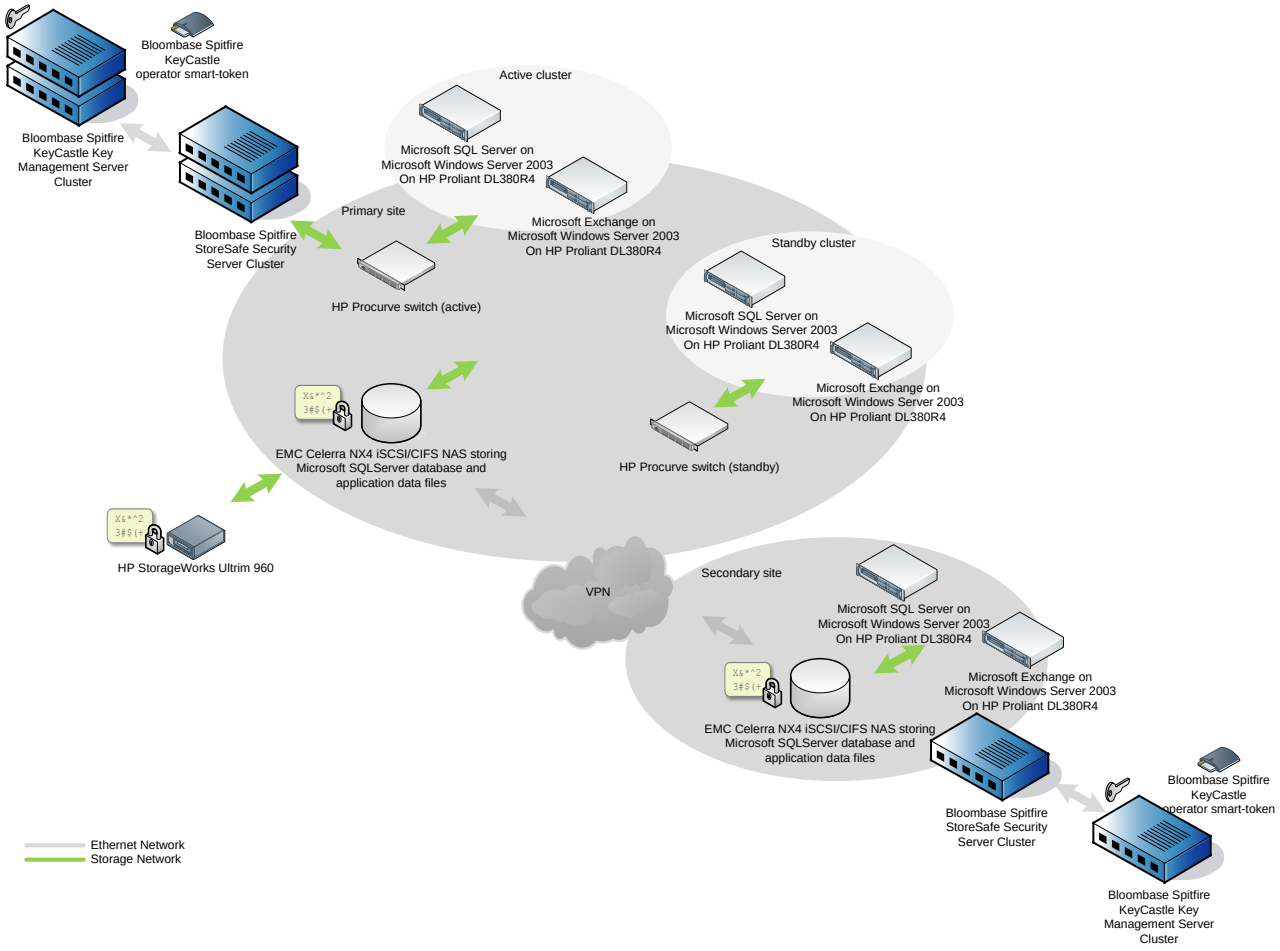
Bloombase High Availability Suite brings together dual Bloombase security servers as a cluster such that when active node fails backup node picks up and maintains non-stop mission-critical service at complete storage and host transparency requiring virtually no operator attention.

Extending to disaster recovery infrastructure, storage cipher-texts at primary site are replicated in their natural encrypted form over private network to backup storage system at secondary site, secured by replica of Bloombase StoreSafe and KeyCastle servers.

FOR MORE INFORMATION

To learn more about Bloombase information security compliance solutions, contact your Bloombase sales representative, or visit:

www.bloombase.com



BLOOMBASE®

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