CUSTOMER SPOTLIGHT

A Government Border Control Agency

Bloombase® Spitfire StoreSafe™ Storage Security Server

Bloombase® Spitfire KeyCastle™ Key Management Server

Government organization secures privacy of sensitive personal border control data of a data warehouse system using Bloombase® Spitfire StoreSafe™ storage encryption and Bloombase® Spitfire KeyCastle™ key management security solution

AT A GLANCE

ABOUT THE CUSTOMER

- Government agency controlling border entrance of people and issue of personal identification and travel documents
- Employees: More than 12,000

SUMMARY

To protect privacy of sensitive personal information of an off-the-shelf business intelligence and reporting system according to regional personal data privacy laws

KEY CHALLENGES

- No change to end user, administrator and operator workflow
- No significant degradation of system throughput and response
- Off-the-shelf data warehouse system cannot be altered
- No coding required
- No hardware, system and application change
- Deployment and data migration can be committed in phases
- Supports storage media including SCSI disks, magnetic tapes and virtual tape libraries (VTL)
- Protects cooked and uncooked/raw filesystems with a single solution

PROJECT OBJECTIVES

- Encrypts dynamic database data stored in storage area network (SAN) and backup tapes
- Protects filesystem objects, relational databases, uncooked volume and backup media
- Interoperable with existing information lifecycle management (ILM) system for automatic data persistence

SOLUTIONS AND SERVICES

- Spitfire KeyCastle™ key management server
- Spitfire StoreSafe™ enterprise storage security server

WHY BLOOMBASE SOLUTIONS

- Enabled customer to leverage existing hardware and software
- Provided comprehensive key and encrypted storage management
- Platform and application neutral
- Scalable and extensible
- Custom cipher support

IMPLEMENTATION HIGHLIGHTS

Was first organization in public sector to institute an end-to-end persistence data protection from data extraction, transform and load (ETL), data warehousing, reporting, backup and archival

KEY BENEFITS

- Immediate information privacy regulatory compliance
- Transparent deployment
- High encryption performance
- No system response degradation
- Highly available and fault-tolerant

EXISTING ENVIRONMENT

- No data encryption in place
- Physical isolation of system hardware in data center

HARDWARE

- IBM p-Series servers
- EMC Symmetrix SAN
- Brocade FC SAN switch
- IBM tape library
- HP Integrity Server

OPERATING SYSTEM

- IBM AIX 5.3
- Redhat Enterprise Linux 4

SOFTWARE

- IBM OnDemand Content Manager
- IBM DB2 Universal Database
- IBM Tivoli Storage Manager (TSM)

Overview

A border control government organization runs an intelligence system to keep track of entrance and exit of people for collection and analysis of movement habits of travelers.

According to personal data privacy laws, such intelligence information are under strict control and required to be secured by strong encryption for all at-rest data on storage media including hard disks, optical disks, magnetic tapes, etc.

Working under tight time constraints, the customer is required to implement effective data protection measures of the system, which has been in operation for 5 years, in within 3 months' time. With stringent constraints including no change to system infrastructure and user/operator workflow as well as the requirement to maintain the same level of service (system response, availability, capacity, etc), end customer selected Bloombase® Spitfire StoreSafe™ enterprise storage security server to provide on-the-fly encryption of their sensitive persistence data and Bloombase® Spitfire KeyCastle™ key management server for full lifecycle management of their cryptographic keys.

An Ambitious Trial Project

The business intelligence system has been in operation for more than 5 years. Like many core business operations systems in the IT infrastructure of this customer, the system is mission-critical.

BLOOMBASE®

As a pilot project for data protection, the encryption solution has to prove fault-tolerant, highly available and disaster-recovery ready.

Border traveler information are submitted to the system timely around the clock which contains sensitive personal information including travelers' names, personal identification numbers such as identity card numbers, visa numbers and passport identifiers etc., date and time of gate-in and gate-out, etc. Such information are collected from various border control units from within the whole state and temporarily stored at a staging storage area of the system. An extraction-transform-load (ETL) worker processes the staging area for incoming traveler information. The ETL worker triggers a content filter to scan for potential hazards. Viral and malicious contents are rejected and moved to parking area for examination or disposal. Clean files are parsed, contents extracted and loaded into a relation database system powered by IBM DB2 Universal Database System.

End users of the system define reports to be run and at what timely manner via IBM OnDemand Content Manager management console. Whenever an analysis task is executed in the system, a report file will be generated and stored at an uncooked storage area managed by IBM Tivoli Storage Manager (TSM). IBM OnDemand Content Manager links the analysis task to the physical disk location(s) where the output reports are stored. On user's retrieval of analysis results, Content Manager reads the physical EMC storage area network (SAN) disk and presents the information to users in a readable form, or as files to be exported for further analysis or reporting use.

IBM TSM manages information lifecycle of the storage area by automatically offloading outdated or less frequently accessed reports to tape libraries for archival, freeing up fast disk storage space for new and frequently accessed reports. On the other hand, if user retrieves a report that OnDemand finds archived, TSM will be triggered to restore the report contents from backup tapes back to SAN disk for user's retrieval.

"Bloombase Spitfire™ enterprise security solution brings you key management, file protection, database protection, raw disk encryption and backup encryption in a single solution at low

Thanks to IBM OnDemand Content Manager, DB2 UDB and TSM, the intelligence system works seamlessly and at the best performance one could get from an IBM Power platform fueled with EMC Symmetrix SAN. However, when talking about data protection, customer faces their first challenge. The application is built on off-the-shelf products that cannot be altered, therefore, there is no way one can introduce data cryptographic processing at the application level.

Customer hit their second challenge when they stepped backward and considered database encryption. Despite database encryption's difficulty on deployment and the vast amount of database objects to get encryption configured, database encryption products cannot solve data privacy problems on the incoming sensitive staging storage and the report repository.

To customer's biggest frustration, their proof-of-concept tests on filesystem encryption products did not work out either. Yes, filesystem encryption works fine with incoming data staging storage, database files and log files, however, filesystem encryption failed to work with the report repository where the filesystem is uncooked, in other words, raw or no filesystem.

Customer did not prefer extra software to be installed on their AIX application servers due to their server capacity and audit requirements. The average processing time for report generation has to be kept within 30 seconds.

Turning Challenge into Opportunity

Apart from support issues of various encryption products end customer considered, there were a number of issues remained unsolved: an all-in-one cryptographic key management system, a scalable encryption platform that can scale up easily as to cope with growing needs of the system, a cryptographic platform that supports a rich set of ciphers and in some special occasions, customer's proprietary cipher algorithms, last but not least, platform independence and application independence to support potential future change of platform.

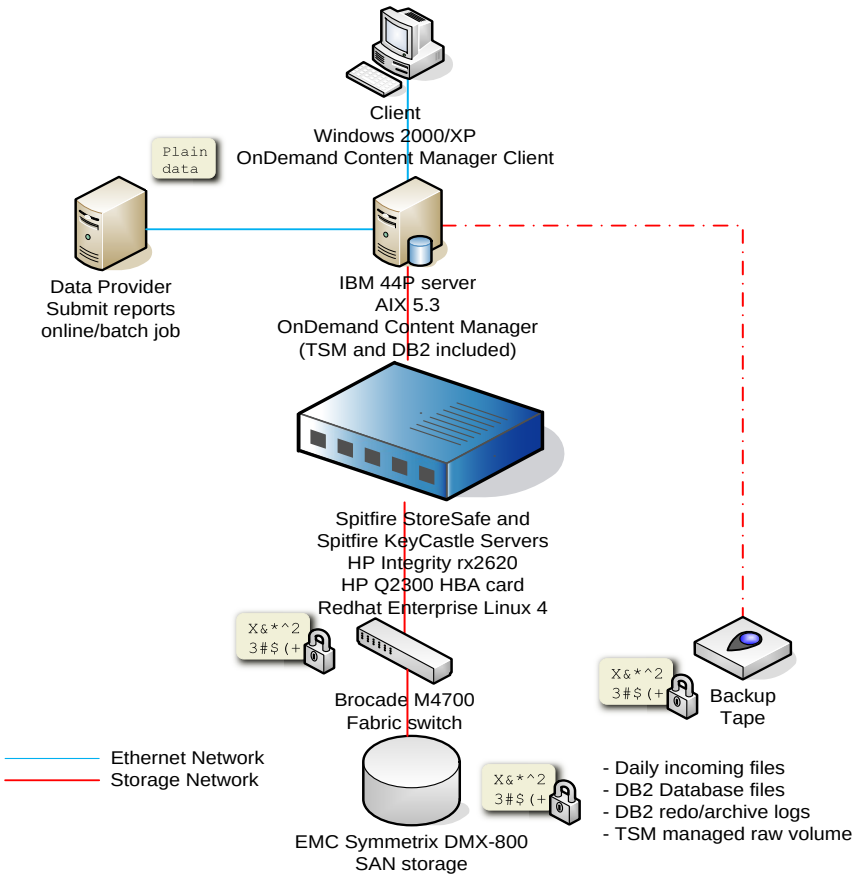
End customer finally turned to Bloombase® Spitfire™ enterprise security solution installed onto HP Integrity Servers to meet their stringent security requirements.

Without the need to alter any of end users' workflow, application and hardware platform, Spitfire StoreSafe™ virtualizes incoming data staging storage, DB2 data file repository and OnDemand Content Manager report repository as Spitfire StoreSafe™ file-based and block-based virtual storages.

Spitfire StoreSafe™ virtual storage offers a secure virtual plain updateable view of the their encrypted contents replica physically persisted on disks. Thus, system and application remain unchanged and access Spitfire StoreSafe™ secured storage contents as if they are normal files and disks, but in reality, the sensitive data are secured by strong encryption. Only when OnDemand Content Manager and DB2 UDB request for storage contents will trigger Spitfire StoreSafe™ to decrypt the ciphered sensitive data and when data are stored by Content Manager or database records committed to DB2 will trigger Spitfire StoreSafe™ to encrypt the sensitive contents before they are physically written to EMC SAN disk.

Spitfire StoreSafe™ enabled the customer to migrate their whole data storage in phases minimizing cutover windows and thus service availability. TSM managed encrypted raw volume as normal volumes without change with benefit that data archived to backup tapes are in their original secure ciphered form.

End customer enjoyed end-to-end data privacy using Bloombase Spitfire™ security platform meeting the toughest national data security requirements at low total cost of ownership (TCO).



4AA0-0696EEP 09/2006

BLOOMBASE®