Bloombase Transparent Data Security: Application Transparent Non-Disruptive Data At-Rest Encryption for Dell Compellent Storage Area Network (SAN) and EqualLogic Network Attached Storage (NAS)

This Technical White Paper provides how organizational customers can meet regulatory compliance and data privacy requirements easily and cost-effectively in real world heterogeneous storage environments by leveraging Bloombase data at-rest encryption software running on Dell PowerEdge servers.

BLOOMBASE®

DELL Technology Partner

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, people and events depicted herein are fictitious and no association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Bloombase.

Bloombase may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Bloombase, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

This document is the property of Bloombase. No exploitation or transfer of any information contained herein is permitted in the absence of an agreement with Bloombase, and neither the document nor any such information may be released without the written consent of Bloombase.

Document No.: BLBS-TN-Bloombase-Transparent-Data-Security-For-Dell-Compellent-EqualLogic-USLET-EN-R2

Table of Contents

Executive Summary

This document outlines the use case scenarios of implementing Bloombase non-disruptive application transparent storage encryption solution on Dell PowerEdge servers securing sensitive at-rest data at Dell Compellent Storage Area Network (SAN) over Fibre Channel Protocol (FCP) and Dell EqualLogic Network Attached Storage (NAS) over Internet Small Computer System Interface (iSCSI).

Bloombase worked with and under the support of Dell Global Solution Labs to evaluate real world use cases of at-rest data protection and additionally, validate the use of Bloombase StoreSafe storage security server to enable Fortune Global 2000 scale organizations to meet data protection regulatory compliance standards easily and immediately.

The Challenge

Traditional IT security studies regard outsiders as origins of cyber-attacks. Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), content filters, anti-virus, anti-malware, anti-spyware, SSL-VPN, Unified Threat Management (UTM), etc all sits at the frontline defending core IT infrastructure at the perimeter only.

Data breaches see a worsening trend in terms of spread and scale, despite the numerous IT security measures deployed and best practices implemented. No matter data exposure is caused by hardware theft, backup tape loss, viral attacks, malwares or insider threats, etc, one could have stopped hackers from walking away with the sensitive data and avoided massive data exposure if having the critical data protected by encryption in the first place. A study by IDG says clearly a lost data record costs an enterprise US $200 for claims, remedial procedures and aftermath.

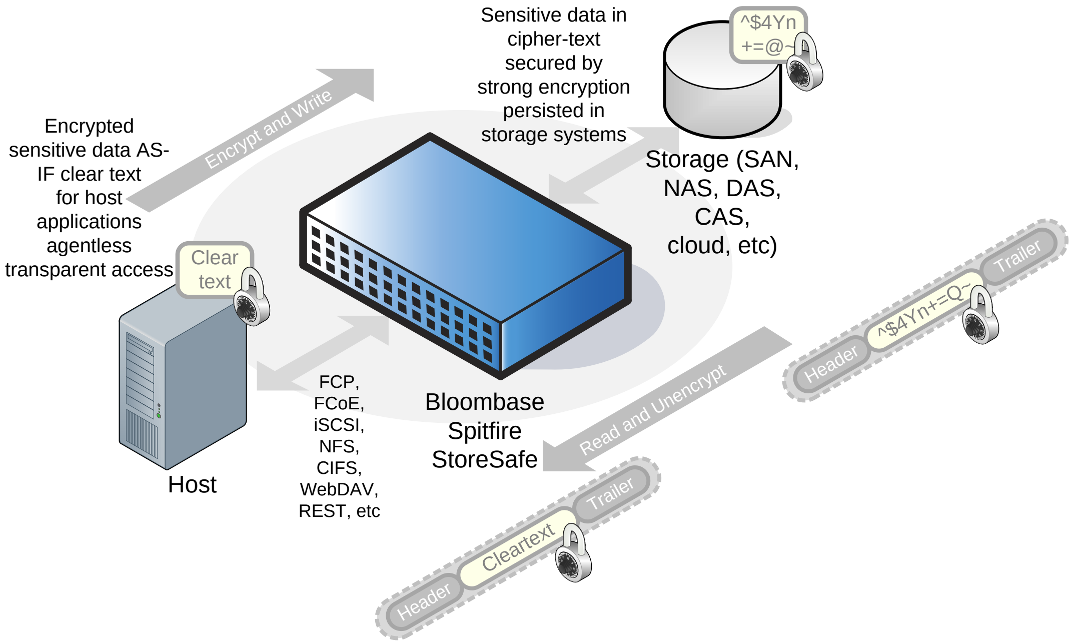
As unknown attacks, insider threats and targeted attacks are on the rise, sensitive and invaluable business data residing in plain on core enterprise storage sub-systems leaves computing and business automation systems in huge vulnerabilities. Encryption of at-rest data is generally perceived as the last line of defense as inked in numerous industry best practices. Nevertheless, enterprises adopting application-specific encryption usually have to pay tremendous efforts on implementation and push the mission-critical applications towards degraded performance and increased risks. The demand for application transparent data at-rest encryption solution and the drive for various information regulatory compliance which has to be high performance, easy to deploy, effortless integration, extensive infrastructure support, sustainable, scalable and fast to deployment as a turnkey solution drives the creation of Bloombase.

Overview

What is Bloombase Transparent Data Security?

Bloombase was created with the mission to address data at-rest leakage vulnerability. Bloombase's goal to put clothes on the naked enterprise critical at-rest data and enable data owners to change easily and securely. Bloombase provides high performance at-rest data encryption software for application transparent unified critical data protection in enterprise information persistence environments from endpoint, through datacenter, to the cloud. Bloombase data protection solutions stand out as independent, versatile, unified and powerful standard-based interface for organizations to secure their complex heterogeneous enterprise application and storage infrastructure easily, risk-free and cost-effectively.

Essentially Bloombase StoreSafe agentless unified storage encryption security solution performs as storage proxy running as a bump-in-the-wire configuration providing transparent encryption and un-encryption of contents stored in enterprise Network Attached Storage (NAS), Storage Area Network (SAN) and RESTful object stores for authorized hosts and applications.


Sensitive data in cipher-text secured by strong encryption persisted in storage systems
^$4Yn +=@~
Encrypted sensitive data AS-IF clear text for host applications agentless transparent access
Encrypt and Write
Storage (SAN, NAS, DAS, CAS, cloud, etc)
Clear text
Header
^$4Yn+=Q~
Trailer
Host
FCP, FCoE, iSCSI, NFS, CIFS, WebDAV, REST, etc
Bloombase Spitfire StoreSafe
Read and Unencrypt
Header
Cleartext
Trailer

Unlike traditional data at-rest encryption offerings in the market which take the form as closed and proprietary hardware appliances, Bloombase assumes a transformative open approach to provide real-time encryption of enterprise storage systems by a software-only implementation. Bloombase StoreSafe is ready to deploy on any x86-architecture hardware server appliance.

Extending to the virtual data-center space, Bloombase StoreSafe offers the capability and flexibility to run as virtual appliances on any QEMU-compliant virtual hypervisors securing virtual machine disk data and virtual storage systems.

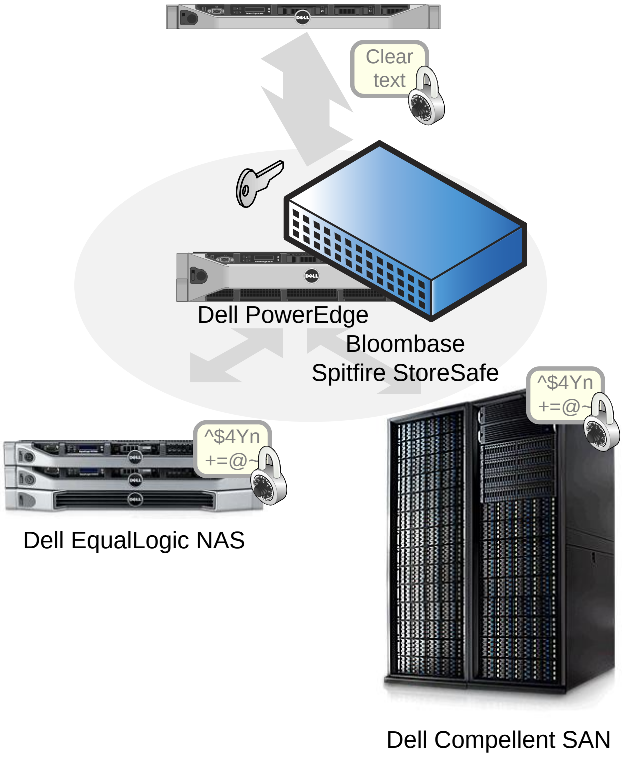
Dell Unified Computing and Storage Platform

Dell offers a complete hardware solution from server computing, network connectivity, storage connectivity, object, file, and block storage infrastructure powering mission critical applications for enterprises of all sizes including:

- Dell PowerEdge rack-optimized servers
- Dell EqualLogic Network Attached Storage (NAS) systems
- Dell Compellent Storage Area Network (SAN) systems

The Solution

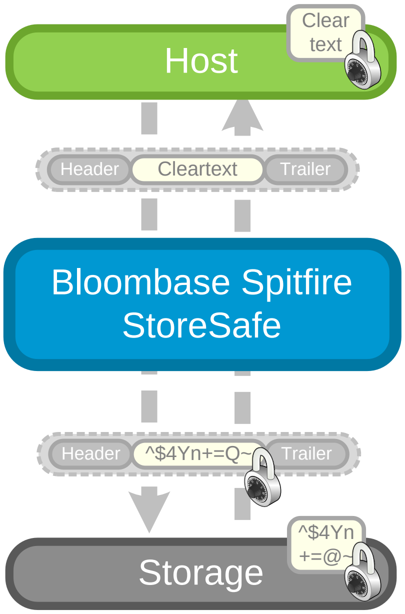
Enter Bloombase data at-rest security software solution, not only Dell provides the high performance and highly scalable compute node PowerEdge servers which Bloombase StoreSafe encryption software runs on, Dell also provides the solid and infinitely scalable storage infrastructure Compellent and EqualLogic systems enabling enterprises to store business-critical sensitive operational data securely and protect these information from unauthorized access by utilizing Bloombase strong encryption technologies.



How It Works?

Bloombase StoreSafe Security Server as a software that is ready to deploy on x86 architecture hardware appliances and as virtual appliances, taking advantage of Dell PowerEdge servers to protect virtually all enterprise data in both physical and virtual data centers. Bloombase StoreSafe at-rest data encryption being fully application transparent and non-disruptive is due to the fact that it operates as virtual storage network resources from DAS, NAS, SAN, CAS to cloud and beyond, enabling heterogeneous applications, hosts and storage systems to interact seamlessly without change.

Trusted applications and authorized hosts leverage virtual storage resources provided by Bloombase StoreSafe to trigger encryption and un-encryption of at-rest data stored at actual storage systems. When host applications store plain-text to actual storage via Bloombase StoreSafe, the Bloombase encryption engine extracts plain payloads and converts them as cipher-text in real-time before they get persisted at the storage media. Reversing the process as hosts read from actual storage through Bloombase StoreSafe, the Bloombase un-encryption engine is triggered to retrieve cipher-text from storage and converts them to virtual plain-text on-the-fly before getting recomposed as plain payloads and presented to host applications.



How It Overcomes the Challenge?

As a matter of defense-in-depth information security best practice, encryption is regarded at all times the last line of defense: even if someone breaks through all other peripheral protection mechanisms and gains access to encrypted data, no one is able to read the hidden information without further breaking the encryption.

Encryption of network in-flight data is trivial and can easily be achieved by open standard technologies such as Secure Socket Layer (SSL) and Internet Protocol Security (IPSec). However, when it comes to encryption of at-rest data, the landscape is a patchwork of piecemeal products, given the diversity of platforms and software, the fact that heterogeneous storage technologies always coexist and the lack of industry standards.

Bloombase pioneers the development of at-rest data encryption by a transformative and extensible unified virtual storage platform that can drop-in to any storage environments easily. Bloombase StoreSafe secures block storage devices (SAN and DAS), file servers (NAS) and object stores (CAS and cloud). Within a single solution, Bloombase is capable of delivering encryption of storage systems supporting protocols including

- Fibre Channel Protocol (FCP), Fibre Channel over Ethernet (FCoE), Internet Small Computer System Interface (iSCSI), and Small Computer System Interface (SCSI)
- Common Internet File System (CIFS), Server Message Block (SMB), Network File System (NFS), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Web Distributed Authoring and Versioning (WebDAV)
- RESTful storage service endpoints

For example, an organization running mission-critical real-time business intelligence applications with sensitive data distributed across the entire IT infrastructure

- information feeds staged at Microsoft Windows Shares at Dell PowerEdge servers
- extract-transform-and-load (ETL) handlers at J2EE-compatible Java application servers
- Oracle Databases at Dell Compellent
- IBM Cognos data warehouses at Dell EqualLogic
- offsite data backup and archive with Symantec NetBackup
- disaster recovery facilities in an all-virtual VMware environment

To meet data privacy and regulatory compliance requirements easily and immediately, customer simply needs to deploy Bloombase StoreSafe unified data protection solution as a single platform to lock down critical operational, backup, archive and replicated data on SAN, NAS, DAS and CAS from physical to virtual data centers effectively.

Integration and Validation

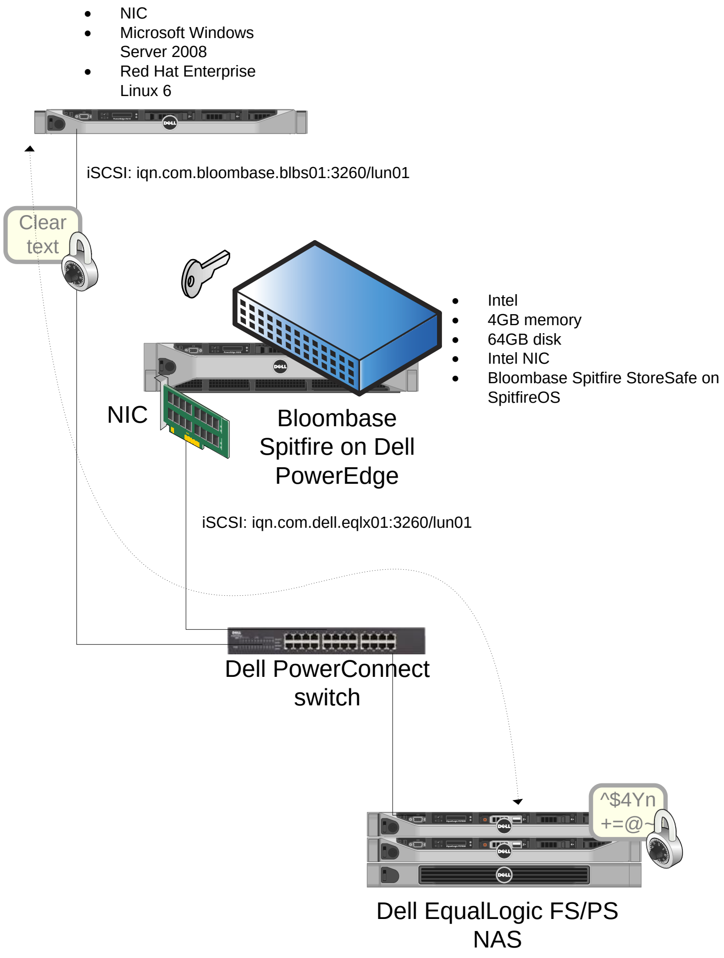
Bloombase StoreSafe's versatility in securing wide range of storage protocols and systems is best illustrated by how it fits seamlessly for SAN/DAS encryption of Dell Compellent and NAS encryption of Dell EqualLogic.

Bloombase Encryption for Dell EqualLogic iSCSI NAS

iSCSI provides the encapsulation of storage SCSI commands over IP networks enabling networked hosts to access block-based storage resources over long distances using existing and next-generation infrastructures. iSCSI storage devices, or targets, are accessed by storage hosts through software or hardware initiators as disk drives. By properly formatting the iSCSI disk drives with relevant file-systems, host applications can access the block storage freely storing and retrieving contents in form of files.

Bloombase StoreSafe Security Server running on stock Dell PowerEdge R710 rack-optimized server provides high performance application transparent encryption of iSCSI targets at Dell EqualLogic NAS. By design, Bloombase StoreSafe operates as virtual iSCSI targets providing encryption and un-encryption of the actual iSCSI disks at Dell EqualLogic. One should expect the Microsoft iSCSI initiator software on Windows Server 2008 host is able to interact with Bloombase StoreSafe virtual targets by iSCSI discovery and connect. As the encrypted iSCSI resource is mounted as local disk drive follow by creation of file-system, applications can read, write and alter file-system objects as-if normal disk drives.

Bloombase StoreSafe on Dell PowerEdge R710 is capable of delivering more than 840Mbps sustained wirespeed in single-threaded real time iSCSI cryptography on Dell EqualLogic. Extending to multi-threaded applications with a maximum of 8 processor-cores to be supported by Dell PowerEdge R710, Bloombase is able to provide more than 6.7Gbps iSCSI storage encryption throughput.

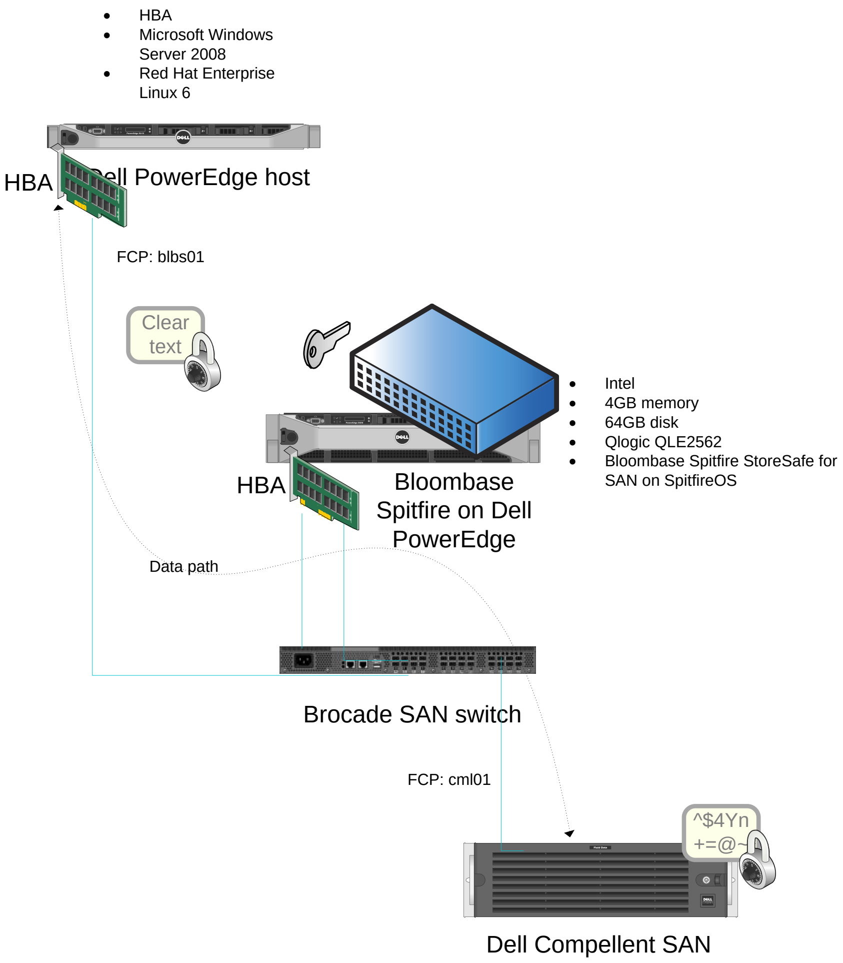

NIC
Microsoft Windows Server 2008
Red Hat Enterprise Linux 6
iSCSI: iqn.com.bloombase.blbs01:3260/lun01
Clear text
Intel
4GB memory
64GB disk
Intel NIC
Bloombase Spitfire StoreSafe on SpitfireOS
NIC
Bloombase Spitfire on Dell PowerEdge
iSCSI: iqn.com.dell.eqlx01:3260/lun01
Dell PowerConnect switch
^$4Yn +=@~
Dell EqualLogic FS/PS NAS

Bloombase StoreSafe encrypted iSCSI targets are fully ciphered such that both file-system objects and file-system render meaningless as if garbage. Anyone gaining access to the garbage-like Bloombase secured iSCSI disk drives has no way of revealing the real secret contents enabling secure at-rest data to be kept private and safe. Microsoft Windows applications such as SQL Server, SharePoint, Exchange, Oracle, DB2, etc leverage Bloombase transparent iSCSI encryption to store sensitive information at Dell EqualLogic NAS with zero change. Adding the benefit that Bloombase StoreSafe is ready to deploy on virtual hypervisors securing virtual machines and virtual storage systems, end result is the ability to meet regulatory compliance requirements cost-effectively and immediately with virtually no change to the existing applications and infrastructure.

Bloombase Encryption for Dell Compellent FC-SAN

While iSCSI provides the transport of storage SCSI commands over IP networks, fibre-channel protocol on the other hand transports SCSI over fibre channel networks. Fibre channel provides low latency communications of storage data for high speed storage area network systems. To be able to access storage resources at SAN, host server appliances have to equip with fibre channel host bus adapters (HBA) and with fibre-channel switches providing connectivity.

Drop in FC-HBAs, in this case QLogic, on Dell PowerEdge R710 running Bloombase StoreSafe, it transforms the powerful rack-optimized general purpose computing node into a high performance FC-SAN encryption server. In this use case, Dell Compellent serves as FC SAN storing encrypted sensitive data to be accessed by Microsoft Windows Server 2008 and/or Red Hat Enterprise Linux 6 hosts with Brocade SAN switch as connectivity.



As Bloombase StoreSafe FC-SAN virtual storage zoning and LUN masking are properly provisioned, authorized hosts can access the virtual-plain LUNs and persist sensitive information as cipher-texts at Dell Compellent as a result of Bloombase transparent FC-SAN encryption. Again, Bloombase virtual storage resources run as normal LUNs for host access. Applications and file systems ride on Bloombase virtual storage interfaces to consume encryption as data is written, and un-encryption when data is read.

Bloombase StoreSafe on Dell PowerEdge R710 with QLogic HBA is capable of delivering more than 1.2Gbps sustained wirespeed in single-threaded real time FC-SAN cryptography for Dell Compellent. Extending to multi-threaded applications with a maximum of 8 processor-cores to be supported by Dell PowerEdge R710, Bloombase is able to provide more than 9.6Gbps FC-SAN storage encryption throughput.

Data encryption at hosts requires drastic application changes which are risky whereas encryption at storage mandates hardware replacement which is costly. In addition, rather than adopting proprietary hardware encryption appliances, Bloombase provides easy to deploy, effortless and cost-effective at-rest data encryption at the core securing Dell Compellent SAN by leveraging general-purpose Dell PowerEdge servers in a fully open and scalable architecture.

Conclusion

Bloombase StoreSafe is a versatile software platform ready to deploy on any virtual hypervisors and any commodity hardware server appliances providing agentless, non-disruptive application transparent at-rest data encryption at SAN, NAS, DAS, CAS and up on the cloud.

In this technical note, Bloombase StoreSafe has been proven fully interoperable on Dell PowerEdge rack-optimized data center computing nodes securing Dell unified storage platforms from iSCSI encryption of Dell EqualLogic to FC-SAN encryption of Dell Compellent.

Customers can rely on Bloombase unified critical data protection solution to protect at-rest data stored at virtually any storage infrastructure maximizing return on investment (ROI) and manageability. As a software offering supporting any general purpose commodity hardware, Bloombase assumes a sustainable solution for operational and archive data which easily live over decades. Not only it protects physical storage and hosts, Bloombase is designed to secure virtual servers, virtual desktop infrastructures and virtual storages making possible data-center virtualization and consolidation, thereby cost savings and ease of management. Bloombase StoreSafe offers rich selection of security features meeting dissimilar security requirements in various industries and nations. It is highly scalable with the hardware it runs on ensuring emerging encryption needs are fulfilled dynamically and efficiently. Bloombase StoreSafe with clustering feature is fault-tolerant and high availability ready for mission critical secure data services. Combining Bloombase KeyCastle or other third party key management tools, it further hardens security and enhances full life-cycle management of keys which is vital to secure deployment of data encryption services. As a low entry barrier turnkey storage data encryption solution at the last line of defense for invaluable critical corporate data, Bloombase guarantees regulatory compliance requirements can be met with least efforts and resources, yet with the best results.

To Learn More

1. Dell PowerEdge Servers, http://www.dell.com/poweredge

2. Dell Compellent Storage Area Network system, http://www.compellent.com/

3. Dell EqualLogic Network Attached Storage system, http://www.equallogic.com/

4. Bloombase StoreSafe Security Server Technical Specifications, http://www.bloombase.com/content/8936QA88Dh3lD3kYMVKxe1VGb8UG4900eNL8Dj

5. Bloombase StoreSafe Security Server Compatibility Matrix, http://www.bloombase.com/content/e8Gzz281s480J2192FF4Btv5HOpb77vLpt1U8V

6. dd for Microsoft Windows, http://software.intel.com/en-us/articles/dd-for-windows/

7. Oracle database server, www.oracle.com/us/products/database

8. Transaction Processing Performance Council, http://www.tpc.org/tpcc/

9. QLogic iSCSI HBAs, http://www.qlogic.com/Products/adapters/Pages/iSCSIAdapters.aspx