



**WHITE PAPER**

# **Encryption: The Business Case for Protecting Data at Rest**



MARCH 2007

# Encryption: The Business Case for Protecting Data at Rest

## CONTENTS

Executive Summary . . . . .	3
Business Requirements for Encryption . . . . .	4
Problem: Adding Encryption . . . . .	6
Solution: Hardware Encryption in Spectra Logic Libraries . . . . .	7
The Encryption Business Solution . . . . .	8
Conclusion . . . . .	9

BlueScale and Endura are trademarks, and Spectra, SpectraGuard and the Spectra Logic are registered trademarks of Spectra Logic Corporation. All rights reserved worldwide. All other trademarks and registered trademarks are the property of their respective owners. All library features and specifications listed in this white paper are subject to change at any time without notice.

Copyright © 2007 by Spectra Logic Corporation. All rights reserved.

## Executive Summary

While network and Internet security have been addressed through rigorous authentication and encryption to restrict access to sensitive personal, financial, and medical information, data at rest remains vulnerable. Restricting access to data backups has been accomplished primarily by restricting access to the backup media. Yet a single backup tape might contain millions of credit card transactions, thousands of medical records, and multiple copies of a company's public and not-so-public financial data. A single backup tape can also fall off a truck, be mislaid in a warehouse, fit in a jacket pocket of a disgruntled worker, or be retrieved by dumpster divers after a tape has been discarded.

Compliance with privacy regulations and explicit legal liability for accidentally exposed information are forcing many organizations to revisit their protection procedures for backup data and media.

Several high profile examples have underscored the difficulty of the fortress approach. Companies with the most data tend to be the companies with the most sensitive data. It's unreasonable to expect that many thousands of backup tapes can be transported, stored, and discarded without a few that end up exposed to misfeasance or malfeasance.

A better solution is to encrypt the backup data, in the same way data is encrypted in network transfers. Like encrypted network data, this gives authorized users easy access while making it nearly impossible for unauthorized users to access data.

Encrypting data prior to storage can be accomplished in several ways, but most have substantive disadvantages in cost, performance, scalability, or management. Spectra Logic Corporation's BlueScale™ Encryption integrates hardware encryption directly into the electronics of a tape library, offering a practical, affordable, and scalable option. BlueScale exploits elements in the modular architecture of Spectra® libraries to provide an easy-to-manage encryption solution.

## Business Requirements for Encryption

A backup tape can contain a treasure trove of information that a network hacker can only dream about: company e-mail, customer databases, support databases, detailed sales and accounting figures, and salary and payroll data—all well-structured, accurate and complete.

Several recent, high profile cases have underscored the exposure and driven new legislation to hold companies liable. These cases include CitiFinancial, Bank of America, and Ameritrade.

Many regulations concerning privacy and protection dictate safeguards on all data, whether on the network or stored on backup media. Many organizations now need or will soon need to comply with one or more of the following:

- ♦ **Payment Card Industry Data Security Standard (PCI DSS)**  
Covers credit card providers and merchants. As of June 30, 2005, Visa requires that any organization that processes more than 20,000 credit card transactions annually (that's an average of less than 55 a day) be certified compliant. The specification suggests: "Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption."
- ♦ **Health Insurance Portability and Accountability Act (HIPAA)**  
Covers health care providers, insurance companies, and company health plans. Encryption is suggested for data security in Section 164.312 (2) (iv).
- ♦ **Gramm-Leach-Bliley Act (1999)**  
Covers banks, brokerages, insurance companies, and financial institutions that receive customer information. Compliance with the data security and privacy provisions of this act requires secure backups (encryption recommended) and data destruction safeguards.
- ♦ **U.K. Data Protection Act (1998)**  
Designates fair practices for the storage and transfer of personal data in the United Kingdom and European Union. Also mandates data destruction: 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'

In addition, California SB 1386, passed in February of 2005, requires that "a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

Organizations may become increasingly liable for data loss and perceived exposure and that organizations that store, transport, or manipulate such data

will want to establish legally defensible practices for security. The protection offered by the NIST-selected Advanced Encryption Standard, AES-256 encryption, demonstrates top-tier compliance in court proceedings.

Even organizations whose main business is not considered sensitive will require PCI DSS certification if the firm performs more than 55 credit transactions a day, or to comply with HIPAA for company health care. All of these are in addition to sensitive payroll, sales, testing, and customer data.

The business case for backup encryption seems clear. However, implementation that addresses this case remains opaque, requiring a solution that overcomes the complexities, cost, and management concerns of encryption. One significant administrative issues associated with encryption is managing the keys used to encrypt data.

Encryption provides huge benefits not only in protecting data at rest, but also in the disposal of backup media. Many of the privacy regulations include the disposal of tapes, while the disclosure regulations dictate the retention period for backed up data. Increasingly, an active management of backups' life spans is key to addressing legal concerns about mandated retention and data disposal. Without encryption, media disposal is difficult; therefore, many firms keep tapes longer than needed or legally prudent. By deleting the encryption key, media is rendered unreadable. With a rotating key sequence, a regular pattern of retention and disposal can be automatically enforced.

## **Problem: Adding Encryption**

Organizations looking to use encryption have typically had two choices: a stand-alone hardware solution or software encryption.

Hardware solutions include Decru and NeoScale appliances. These high-quality, high-performance devices connect in series before the backup device to perform encryption. These devices are chosen because of performance and security. They are currently the only encryption method that is being tested for Federal Information Processing Standards (FIPS) as required in high-security governmental organizations.

The drawbacks most frequently cited to this approach are: significant cost; scalability concerns in that new encryption devices must be added as tape drives are added; and management concerns since these stand-alone devices require a great deal of administrative overhead.

Software encryption, conversely, is available on many operating systems and on many backup software applications for free or for little cost. The problem with deploying this in a large enterprise is performance.

Software encryption is extremely CPU intensive. Unless a large amount of unloaded CPU resources are available at backup time, this solution works marginally at best; even if resources are available, the throughput loss frequently prevents a tape drive from streaming during backup, which can exacerbate performance problems and, over time, jeopardize the reliability of backups and the devices used to create them.

Decrypting data is just as CPU-intensive as encrypting it. Performing software encryption and backup in off-peak hours still leaves performance issues unresolved for software-based decryption and data restoration, which is not necessarily done during off-peak and is frequently time-critical.

Depending on the software used, very little support is available for key management. IT staffs are left to develop their own procedures for creating, saving, storing, and expiring encryption keys—as well as transporting them to the device or server.

Spectra Logic's BlueScale encryption technology addresses all of these concerns, providing effortless and cost-effective hardware encryption built into the tape library used for backup.

## **Solution: Hardware Encryption in Spectra Logic Libraries**

Spectra Logic libraries are built using a modular architecture, developed to facilitate upgrades to technology and to provide scalable capacity and performance. The key factors that relate to encryption are the libraries' modular architecture and BlueScale environment.

Spectra libraries use modular controllers—Quad Interface Processors, or QIPs—that handle connectivity with the wider network. These modular components can be added incrementally. The BlueScale environment supports an easy-to-use interface available across multiple libraries, and Shared Library Services—SLS—that lets a single library function as multiple separate libraries through partitions. Each SLS partition presents itself to a host as a distinct, disparate library with dedicated drives and tape slots.

With BlueScale encryption, data is protected through an encryption microprocessor on the modular QIP. Using the common interface, users set up specific partitions (all or any) that will be assigned to encrypted data. The administrator uses the common interface to create a key and assign it to one or more partitions—and if the library has only one partition (by default, every Spectra library does), and a key is assigned to it, then all data backed up through that library is encrypted.

Implementing encryption in the QIP provides a highly scalable solution for encryption as total throughput is not limited by CPU bandwidth, as in a software solution, nor by a limited number of stand-alone encryption devices.

The common interface provides access to all of the key management features using the Endura™ Key Management application. This application centralizes key management and supports all aspects of key management, including creating keys, assigning keys to partitions, exporting keys (for secure storage) and importing them again.

Another option is available for remote management of encryption through a Web-based Remote Library Controller application, secured through Secure Socket Layer (SSL). If this is appropriate for a site, administrators can manage both the library and encryption from anywhere.

## The Encryption Business Solution

Including encryption in the tape library overcomes most of the complexities of an encryption strategy. To retrofit a traditional library to provide encryption on some drives and to manage keys would be difficult. The extensible architecture of Spectra Logic libraries includes the required components. Upgrading or adding a modular encryption-enabled component (QIP) to a Spectra T120 or T950 library, and upgrading library firmware are all that is needed to upgrade a Spectra library.

BlueScale encryption implements AES-256 in Spectra Logic libraries. The length of the encryption key is 256 bits. This is the government standard accepted by the National Institute of Standards and Technology as “a [Federal Information Processing Standards] FIPS-approved symmetric encryption algorithm that may be used by U.S. Government organizations (and others) to protect sensitive information.” Without the key, AES-256 encrypted data is considered unrecoverable.

## Conclusion

Encryption of backup media will continue to escalate in importance over the next few years. The need for encryption has been constant, but only now, with BlueScale Encryption, have the implementation challenges been overcome.

It's difficult to imagine a public or private organization that does not routinely back up sensitive data about its finances, employees, customers, technology, or communications. The risk of this information getting into the wrong hands because of a misplaced or stolen tape is potentially disastrous for the organization.

As organizations look to implement encryption, storage-based hardware encryption makes the most sense. Host software applications lack the performance to encrypt all data, and interconnect devices are typically too expensive for all but the most secure installations.

Spectra Logic's library architecture puts the company in a unique position to integrate encryption and Endura key management. With BlueScale Encryption, Spectra Logic (in part by working with NeoScale) can meet customer security needs that range anywhere from basic organizational privacy to government facilities that require the highest levels of FIPS compliance.

By including BlueScale encryption in the tape library, all backed up data can be encrypted. Different backup software, heterogeneous networks, direct-attach, SAN, and NAS storage can all take advantage of high-performance AES-256 hardware encryption using existing tape drives and formats.

The configurable, scalable, Spectra Logic libraries give customers an integrated encryption solution, with comprehensive key management features, is described in greater detail in another Spectra Logic white paper. Even libraries purchased before encryption was available can be upgraded with a simple field-replaceable components and a firmware upgrade.

Tape drives may encrypt data as future generations of drives are released, just as data compression has become a standard drive feature. Spectra Logic remains committed to protecting customer data and will integrate new technology, such as tape drives that encrypt data, as it becomes available.



Spectra Logic Corporation  
1700 N 55th Street  
Boulder Colorado 80303 USA  
800.833.1132  
303.449.6400

Spectra Logic Europe Limited  
Magdalen Centre  
Robert Robinson Avenue  
Oxford Science Park  
Oxford UK OX44 7 RW  
+44 (0) 870.112.2150