

WHITE PAPER

**Case for Router-Based Encryption
Comparison of Tape Encryption Options**



READVERIFY APPLIANCE (RVA) OVERVIEW

It is now a common belief that removable media, at a minimum, needs to be encrypted before it leaves a company's facility, and in many cases, as media is created. Since the beginning of the digital age, there have always been security risks. However, since the amount and importance of data has grown year after year, securing this information has become more critical to all organizations. The challenge for the IT department is one of focus: Do we secure all of the data going to tape, or do we isolate data based on relative importance and protect only that information? These questions are important in answering what type of security solution is adequate. Before discussing the best options for specific environments, this paper will first describe the different options for tape encryption in the market place today: host based, appliance based, router based, switch based and device based.

Encryption Method	Vendors
Host	Symantec, EMC, HP, IBM, CommVault
Appliance	NeoScale, Decru
Router	Crossroads
Switch	Cisco, Maxxan
Device	LTO4 (IBM, HP, Quantum, Tan-berg) T10000 (SUN)

HOST-BASED

Host-based encryption has been available in the market the longest and provided by many of the top backup application vendors. The benefit of performing encryption with the backup application is one of granularity and control. Since the data being backed up is configured and setup through the backup application, adding an encryption step is a simple addition to the process.

There are downsides to this approach as well. Many applications don't provide for data compression before encryption and those that do come with a significant performance impact. Since encrypted data can not be compressed, the tape drive compression benefits are lost; therefore, the amount of data being stored on the tape medium will be cut in half or more if compression before encryption does not occur. The backup server is already a critical performance element where many systems are not capable of keeping data streaming to tape drives or utilizing the tape system efficiently. Adding the processing-intensive functions of

CASE FOR ROUTER-BASED ENCRYPTION

compression and encryption will only serve to exasperate any performance or utilization issues in the overall system.

Additionally, the key management approach to host based encryption has not met government or enterprise level requirements. It is different for each system, but typically the generated keys are reused and not securely stored. Also, the keys can be accessed by the same resources that are performing the backup application maintenance and are tracked via secure logs.

APPLIANCE BASED

Appliance based solutions appeared next in the market about three years ago. This approach was to improve on the host based solution, providing the compression and encryption in a dedicated hardware system that sits in the data path post the backup application and pre the tape devices. The benefit over the host based was clearly in performance, and these solutions also brought the enterprise level key management that government and major corporations demand for a long term solution.

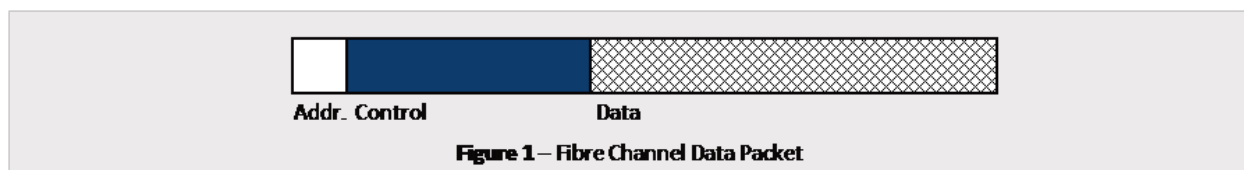
The challenge in these solutions is their price/performance and overall network position. While these solutions solved the key management and compression issues with the host based products, they come with such a significant cost that many corporations are being forced into solving their encryption issues by the second method mentioned above—isolating data and only encrypting that information. This might be a viable method, but some businesses or agencies might find it too constrictive to meet their overall objectives. Part of the problem for these solutions still centers on performance. The challenge is that tape devices are continually improving in their throughput and therefore, in their minimal streaming rates. If the tape drive isn't kept streaming, the overall performance of the backup will actually go significantly down as the drive is forced to continually backup and restart. This also has the adverse effect of potentially damaging the media and causing permanent data loss. Therefore, these appliances must have enough throughput to keep the attached tape devices streaming. Unfortunately, this approach causes the need for significant processing power, which translates to heat and associated increase in cooling. While this doesn't seem significant for a single box, it adds up quickly when it is determined that these systems are barely capable of streaming an LTO3 drive (per each output port) and can just keep two LTO2 drives streaming. When a complete environment is considered, the number of encryption appliances becomes significant. Therefore the cost/performance comes into play along with the wattage/heat requirements as well.

Secondly, since these appliances are in the data path, significant networking challenges are created. The appliance must terminate the transmission from the host and re-initiate it with the device. This now brings in the requirement to interoperate with not only the different types of tape devices, but also the switches, HBAs, Servers and backup applications. Unfortunately, all manufacturers of those products interpret the SCSI and FC standards in their own way and therefore each configuration can create a non-operative environment for

the appliance. There are also many devices still in use today that were created under different versions of the standard and do not operate the same as the newer devices on the market. There are many know cases where the appliance vendors state they will not support certain devices or host systems. There are many know cases where the appliance vendors state they will not support certain devices or host systems.

ROUTER BASED

The first (and only to this point) router based encryption solution was introduced by Crossroads Systems in April of 2007. This solution was built on the existing router platform that is currently connecting well over 300,000 tape devices in the market today. To better understand the difference in a router based approach, it is best to describe what a switch does versus the router. Figure 1 shows a data packet as it is sent from the host. A switch will only look at the address (Addr) bits to determine where the data packet needs to go. This is very few bits and can be accomplished with great speed thus making the fabric very efficient. A router looks at the control data along with the address and determines not only where the data needs to go, but also what needs to be done with the data as well. This requires the router to terminate the transmission and re-initiate it based on the knowledge it gained from the control data. As an example, in the case of protocol bridging, the router would terminate the fibre transmission and re-initiate it as a parallel SCSI transmission to SCSI based tape drives.



Terminating and re-initiating the data is the same requirement that the appliance based approach must take, but with the router there are some significant advantages. First, the router core (a high performance, low latency routing layer) replaces the standard I/O stack that are in servers. This routing core enables the data to be copied once before it is re-routed to its destination. This results in significant performance improvement over the appliance based approach. Also, in the 10 years of product life, Crossroads has developed quality of service and error recovery mechanisms at the network layer. These include methods for keeping data flowing from the host (immediate data response, and response caching), bit error recovery (Crossroads invented and created the FC standard for recovering from a bit error in the data transmission which is critical in a tape environment where a single bit error would cause the backup to fail), and Access controls which give the user many of the granular controls for which data to encrypt that the host based solutions provide.

All of these culminate with a significant price/performance advantage for the customer. The Crossroads TapeSentry 4f gives the user the ability to connect 12 LTO2 drives or 6 LTO3 drives,

CASE FOR ROUTER-BASED ENCRYPTION

keeping all streaming. The TapeSentry is list priced better than the cheapest appliance solution and truly shows its scaling when multiple systems are required. In two different head to head comparisons, the required number of TapeSentry's was one-half in one case and one-third in another. This not only resulted in hundreds of thousands of dollars in systems cost, but also greatly reduced the power and cooling requirements to encrypt their environments.

Since the TapeSentry is built on the router platform that has been in production and shipping for more than 10 years, it benefits from the industries most interoperable solution. The routing platform has connected every type of server, HBA, switch, and device in the market. It has solved issues with host systems like Non-Stop servers, iSeries, OpenVMS, and Unisys platforms—along with connecting all varieties of SCSI and FC based tape devices.

TapeSentry also brings the same level of enterprise key management that the appliance based solutions provide. This includes multi-level encryption, encrypted logs, encrypted key database, and automatic key backup. Additionally, the TapeSentry was designed to work with third party key management systems. While it is everyone's desire to develop of key management standard, it is our belief that this won't occur in the timeframe required by many businesses, and having a system that is flexible to work with the choices the customer makes will provide the most flexibility for the user.

SWITCH BASED

Switch based solutions have been announced by many vendors, but at this time it is difficult to measure their performance in production environments and not much is documented on their approach, but it is a fact that they must be taking either the appliance or router approach. Since they are switch vendors, they are stating this as “switch based” or “fabric based” encryption. Again, a switch only looks at the address of a packet, but to perform compression and encryption the whole packet must be terminated. This means that this solution has the same level of concerns that the appliance or router based solutions have—price/performance, networking and interoperability.

It is tempting to believe that a switch based solution will solve the interoperability issues since many of these vendors have been providing switches, thousands of them for years. However, the interoperability issues do not exist at the same level with switches. Since most of the interoperability issues result from hosts, HBAs, or devices interpreting SCSI commands, the switch is isolated from this since those problems occur in the control data section. Therefore, every switch based encryption solution will face the same interoperability issues that the initial appliance based solutions had to deal with and will probably solve it the same way – limit the supported environment.

While having the encryption in the same box as the switch makes sense from an architecture perspective (minimized boxes, minimized connections), it raises other concerns. Mostly, do

you want your fabric which is controlling your day to day operations having additional functionality that if it breaks could cause your whole environment to go down? The literature states that these solutions will also provide enterprise key management similar to the appliance and router based solutions.

DEVICE BASED

Device based solutions have been coming to market over the course of 2007 from the LTO4 providers and with the SUN T10000 drive. The benefit lies in simplicity and performance. The encryption process is added post the existing compression engine and therefore, every drive now comes fully equipped to perform encryption with no performance loss. The cost of the environment is somewhat obscure in that many manufacturers are saying that encryption is free, but of course you must upgrade to the new drive to get it. It is also unknown how much the key management for the drives will cost. It is also required that the backup application be upgraded to support turning on encryption at the drive.

The downside to drive based encryption is more subtle. The obvious point is that all of the devices must be upgraded, which will come at a significant cost both in systems as well as in downtime. This will also require migration of old media to new in order to fully achieve the new drive benefits. A more subtle issue was discussed earlier. The LTO4 streaming rate is 54 MB/s. Many environments struggle achieving 30 MB/s and therefore upgrading to LTO4 will actually cause a slower environment (as the drive reverses and restarts) and will more than likely damage media as well. There are unknown costs in the backup application upgrades and the key management that must be accounted for as well. Next, by using the device based approach the customer is locked into that device and that manufacturer. The device is no longer a commodity where best pricing and service can be negotiated for every purchase. Lastly, this requires that all devices are upgraded or once again the IT administrator is forced into making the decision to isolate certain data and only protect that set.

CONCLUSION

There are many viable options to provide encryption for removable tape media on the market today, with new announcement from vendors almost every month. This paper started by stating that the appropriate solution is somewhat dictated by the users environment and their desires: Do we secure all of the data going to tape, or do we isolate data based on relative importance and protect only that information?

If isolation of data is the approach then most of these solutions compete favorably. Choose host based if performance or tape usage isn't an issue. Choose device based since the upgrade will be limited and focused on that data set. Choose appliance based since the environment can be controlled to systems they interoperate with and lower performance drives can be used to maximize connections, or choose router based since it will interoperate with the environment and connect the devices of choice. The decision will need to be based on other factors such as overall cost, flexibility of solution, and vendor support.

CASE FOR ROUTER-BASED ENCRYPTION

If securing all of the data or a significant portion of it is required then the solution options become fewer. In many cases the device based won't solve the problem since many hosts can't connect to the new devices or the user simply doesn't have the budget to replace LTO3 or LTO2 drives that they might have bought just last year. The host based solution is challenged as well—due not only to the weak key management, but also to the fact that many environments have multiple backup systems and having a mixture of encryption solutions based on backup applications would be daunting to manage. This leaves the appliance and router approach. The challenge for the appliances is their limited interoperability and performance which causes a significant cost increase over the router based solution.

It is our belief that the router based solution is not only the best solution for the user that has heterogeneous and diversified backup requirements, but will also provide the best solution for the user that has only a limited data set to be protected. The router based solution provides the industries best interoperability, combined with price/performance advantages to every solution on the market.



Crossroads Systems, Inc.

11000 North MoPac Expressway
Austin, Texas 78759
USA

TEL: 866.BUY.CRDS
866.289.2737
512.349.0300

FAX: 512.349.0304

EMAIL: sales@crossroads.com

www.crossroads.com

Crossroads Europe GmbH

Marie-Curie-Str. 19
73529 Schwäbisch Gmünd
Germany

TEL: +49 7171 99800-0
+800 46243726

FAX: +49 7171 99800-10

EMAIL: contact-europe@crossroads.com

ABOUT CROSSROADS

Headquartered in Austin, Texas, Crossroads Systems delivers flexible solutions to protect, secure and restore business-critical "data-at-rest." Crossroads (symbol:CRDS) is currently traded on Pink Sheets and also posts its financial disclosure reports, press releases and other related documentation on the OTCIQ webservice of the Pink Sheets website. For more information, please visit www.crossroads.com.



Crossroads promotes institutional and personal environmental responsibility within the company, with our partners and with the users of our products. We are committed to providing the best products and services while encouraging practices consistent with sustainable living and resource conservation.

© 2008 Crossroads Systems, Inc. Crossroads and Crossroads Systems are registered trademarks of Crossroads Systems, Inc. Specifications may be subject to change.