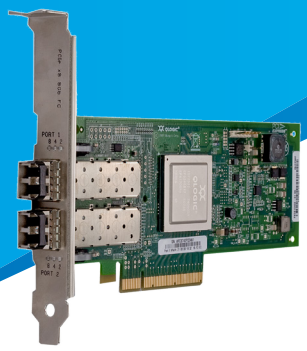
Data-at-Rest Encryption Addresses SAN Security Requirements

QLogic 2500 Series Fibre Channel Adapters Meet Enterprise Security Needs



QLogic Fibre Channel Adapters from Cavium provide a secure solution that works well with SEDs and provides interoperability with other hardware components in the SAN without the need for adapter-based encryption.

EXECUTIVE SUMMARY

Over the years, Fibre Channel SANs have become the backbone for serving the information needs of enterprise data centers. SANs have been traditionally considered physically secure due to their closed and physically isolated location in data centers. While physical network isolation offers critical security, breaches through unauthorized hosts or users still poses potential security risks.

Adoption of server virtualization technologies, increasing the number of physical or virtual servers in data centers, and data center growth through mergers and acquisitions have resulted in increased security concerns. Accordingly, security has remained the top budget priority over the last five or six years, with 60 percent of companies placing it as the highest priority in a recent International Data Corporation™ (IDC) survey.

This paper shows how data-at-rest encryption, when used with physical SAN security and techniques such as zoning and LUN masking, address all the major security risks that are faced by today's IT storage administrators. This paper also shows how encrypting data closest to the media addresses the SAN security risks. Additionally, alternative approaches are discussed, such as fabric encryption, which pose implementation and interoperability challenges that negate pervasive adoption in data centers of the future.

KEY FINDINGS

SAN security via encryption is necessary for protecting data when it leaves a physically secure SAN (for example, tape backups and hard disks leaving for repair or retirement). This paper reveals that:

- Encryption of data at the media (data-at-rest encryption with self-encrypting drives), in conjunction with physical SAN security, addresses all major storage administrators' security concerns. This type of encryption allows for minimal disruption of existing SAN infrastructure deployments and maintains interoperability.
- Alternative approaches to secure data, such as adapter-based encryption, are solutions looking for a problem. These approaches promote vendor lock-in, as the data encrypted by the hardware/adapters can only be read by the same vendor's adapter or proprietary solutions that created them. Such approaches also pose new security risks if interoperability with existing deployments is mandated by IT managers.
- Host-based encryption poses new challenges to data compression or de-duplication applications.
- Fabric based encryption (switch-to-switch) addresses security needs when data is being exchanged between SANs across the WAN. Pervasive adoption of such features requires standards-based key management, which does not exist today. Every vendor's key manager handle keys differently, making interoperability a challenge.
- QLogic® Fibre Channel Adapters from Cavium™ provide a secure solution that works well with Self-Encrypting Drives (SEDs) and provide interoperability with other hardware components in the SAN without the need for adapter-based encryption.

Data-at-Rest Encryption Addresses SAN Security Requirements

INTRODUCTION

SAN security breaches are expensive, costing corporations over a million dollars in recovery charges. In addition, information explosion and server proliferation have caused new challenges for data centers, driving security threats to critical levels. With regulations like Sarbanes-Oxley, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and the California Security Breach Information Act (SB-1386), companies face increasing pressure to retain this information for longer periods of time, while also ensuring its privacy. The cost of security breaches, coupled with emerging business practices and regulatory compliance, creates a new set of challenges for enterprise data centers. A majority of the United States (US) now have data privacy laws stating that encrypted data that is breached does not have to be reported. US congressional bills have similar provisions.

Determining where to protect and encrypt digital assets in the enterprise requires an understanding of the potential threats as well as where the vulnerabilities reside. For the SAN, developing a security strategy requires an understanding of the crucial vulnerabilities in the storage infrastructure and the potential type of threats that arise. This paper segments security threats and data as follows:

- Users
  - Authorized
  - Non-authorized (hackers)
- Threats
  - Unintentional errors (caused by authorized users)
  - Intentional malicious attacks (carried out by hackers and rogue users)

Figure 1 summarizes the techniques used in the SAN to address the security threats posed by both types of users.

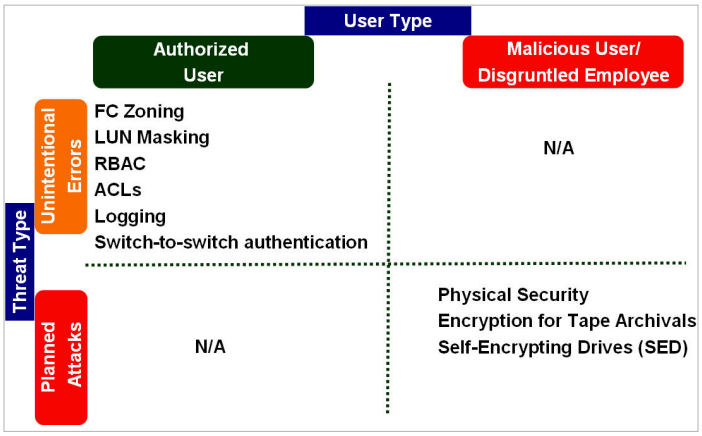


Figure 1. Security Techniques by Threat and User Types

Authorized users such as employees, system administrators, and database administrators may accidentally access sensitive data if the SAN is not secured properly. A typical cause for SAN service interruptions is unintentional errors caused by authorized users.

These types of problems, as shown in Figure 1, are resolved by leveraging common SAN techniques such as zoning, LUN masking, virtual fabrics, Role Based Access Control (RBAC), Access Control Lists (ACLs), switch-to-switch authentication, and implementing controlled IT processes.

In the case of planned attacks by unauthorized users (lower right quadrant of Figure 1), it is well known that Fibre Channel SAN security is enforced through physical means and network isolation. The fact that the Fibre Channel SAN is a separate physical network from the LAN offers the first level of protection. The second level of protection is that the SAN is physically protected against physical access to the data center.

Once physical security is instituted in a SAN, the only security exposure is when backup tapes and disk drives leave the data center. This exposes sensitive data from being accessed by an unauthorized user. It is important to encrypt tapes and disk drives, whether they stay in the data center or are stored outside the organization.

STANDARD SAN SECURITY TECHNIQUES

QLogic 8Gb Fibre Channel Adapters from Cavium deliver authentication through Fibre Channel-Security Protocol (FC-SP) technology. FC-SP is a security framework (defined by the T11 standards group) that includes protocols to enhance Fibre Channel security in several areas, including authentication of Fibre Channel devices, cryptographically secure key exchange, and cryptographically secure communication between Fibre Channel devices. FC-SP protects data in transit throughout the Fibre Channel network.

Diffie Hellman-Challenge Handshake Authentication Protocol (DH-CHAP) is a secure key-exchange authentication protocol that supports both switch-to-switch and host-to-switch authentication. DH-CHAP is a secret-based authentication and key management protocol that uses the CHAP algorithm (see RFC 1994) augmented with an optional Diffie-Hellman algorithm (see RFC 2631). DH-CHAP provides bidirectional authentication, and can provide unidirectional authentication, between an *authentication initiator* and an *authentication responder*. To authenticate with the DH-CHAP protocol, each entity, identified by a unique name, is provided with a *secret*.

QLogic 8Gb Fibre Channel Adapters from Cavium support FC-SP authentication using DH-CHAP protocol. In addition, Cavium has provided software solutions to expose these features to end users. Using DH-CHAP capabilities through Cavium's QConvergeConsole® data center managers can enforce authentication between hosts and switches connected to a Fibre Channel SAN.

SAN management software can limit access by partitioning or segmenting storage resources so that only authorized users or enterprise groups can view certain SAN hardware components. Access control in an Fibre Channel SAN is accomplished through a technology called zoning. Zoning allows users to specify groups of devices that can talk to each other.

Data-at-Rest Encryption Addresses SAN Security Requirements

The primary purpose of zoning is to protect Fibre Channel SAN environments from spoofing attacks, where a malicious system successfully presents itself as a legitimate system and gains access to a protected resource. Zoning can be accomplished through hardware or software, depending on which it is termed: hard zoning or soft zoning.

With hard zoning, also know as port zoning, members of certain zones are allowed to communicate only with certain systems by managing access on a port-by-port basis. The Fibre Channel switch keeps a list of valid port addresses and only allows communication among ports within the same zone. If a port tries to communicate with a port in a different zone, the frames from the non-authorized port are dropped.

Since hard zoning is based on ports, it is more secure and efficient than soft zoning, which uses the World Wide Number (WWN) instead of port numbers. The switch checks the WWNs of the source and destination. Data is forwarded only if the source and destination belong to the same zones. Even though hard zoning is less flexible to manage and configure, it is preferred by SAN administrators because it provides tighter security.

Physical security in a SAN, when combined with standard SAN security practices described in this section, address the major risks faced by customers today.

ADAPTER-BASED ENCRYPTION: A SOLUTION LOOKING FOR A PROBLEM

There isn't a single comprehensive encryption approach that covers all threats to data-at-rest. Therefore, care must be taken when choosing where to encrypt. Data encryption options come in many forms, including host-based software, encryption hardware appliances, and encryption ASICS that reside on the adapter, switch, RAID controller, and hard drive (see Figure 2 below). There are cost, interoperability, performance, and latency issues to consider with each of these options.

Encryption Upstream and Above the Adapter and File System

Encryption at the application, database, Operating System (OS), or file system are all techniques that cover threats for data-in-transit within the different software layers of the host server, addressing potential vulnerabilities that may reside in those layers. Hackers might be able to exploit these vulnerabilities and access sensitive data.

Database vendors provide encryption services in their software that allow selectively securing certain fields of a database. For example, a database may encrypt only credit card numbers and social security numbers; the remaining content of the data base is unencrypted.

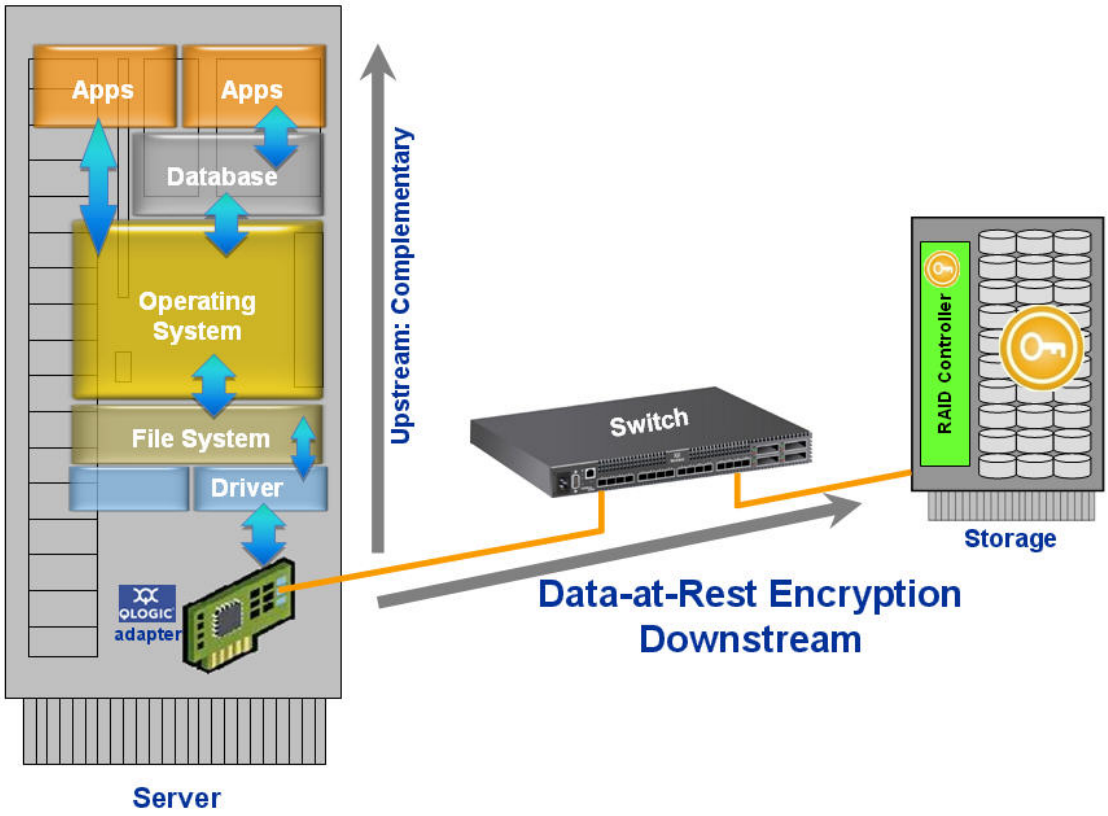


Figure 2. Components In the I/O Path from Host to Targets

Data-at-Rest Encryption Addresses SAN Security Requirements

Due to significant performance degradation, as well as non-scalable changes required to the application, database, OS, or file system, only a limited portion of data is encrypted. Administrators address this issue by encrypting only the most sensitive data. Administrators must rely on data classification to identify this sensitive data and where it exists. It is widely acknowledged that data classification fails to identify all instances of sensitive data. It is difficult, labor intensive, and hard to maintain, especially when the sensitive information can be copied from a protected source to an unprotected destination. This situation means that too much unencrypted sensitive data is written to hard drives; data that will likely persist on the hard drive long after the drive's useful life.

Encryption in the Adapter or Switch

Encryption technologies that are downstream of the file system (starting at the adapter and through the fabric) must provide full disk encryption to fill the gap where data classification fails to capture sensitive data. These technologies relieve the data custodian from having to classify the data when it leaves the control of the data center. Otherwise, the owner would have to know the data sensitivity level to dispose of the drive, which adds more work for management. Encrypting in the adapter and fabric switch are possibilities.

Adapter or switch encryption requires additional equipment such as an encryption engine to scramble and descramble the data and a key manager (hardware appliance or software) to create, manage, and store the encryption keys.

Data-in-flight moving across the wire at the block level on a SAN is not normally considered a security risk when physically protected within the walls of the data center. There are potential risks with FC fabric links that leave the data center and extend the SAN to remote offices, to other campuses, or to remote locations for disaster recovery (see Figure 3). In those cases, security is addressed by using either FC-SP over Fibre Channel, or routing the FC links over Internet Protocol (IP) and protecting the data with IP security. Routers and switches use technologies such as IPSec to protect and link SANs over WANs. To specifically address this type of security threat, host/adapter based encryption is not required as long as the switches and routers support IPSec data encryption.

Fibre Channel technology can only reach a distance of about 10km. IT managers need to share, protect, and move data much farther than that—sometimes across geographic borders. Cavium provides routers and switches that allow SAN traffic to move over IP, linking SANs over WANs.

When IP extends the SAN over the Internet or dedicated lines, IPSec security is used on these remote links to protect valuable data over long distances and to support data replication, SAN data device sharing, and for backup and business continuity.

Figure 3 shows how the SAN is extended over an IP WAN and protected with IPSec to ensure that data-in-flight is secure. Secure Sockets Layer (SSL) sessions are used for the WAN links (with ephemeral keys) to ensure that the link remains secure and that keys are not exposed for long periods of time.

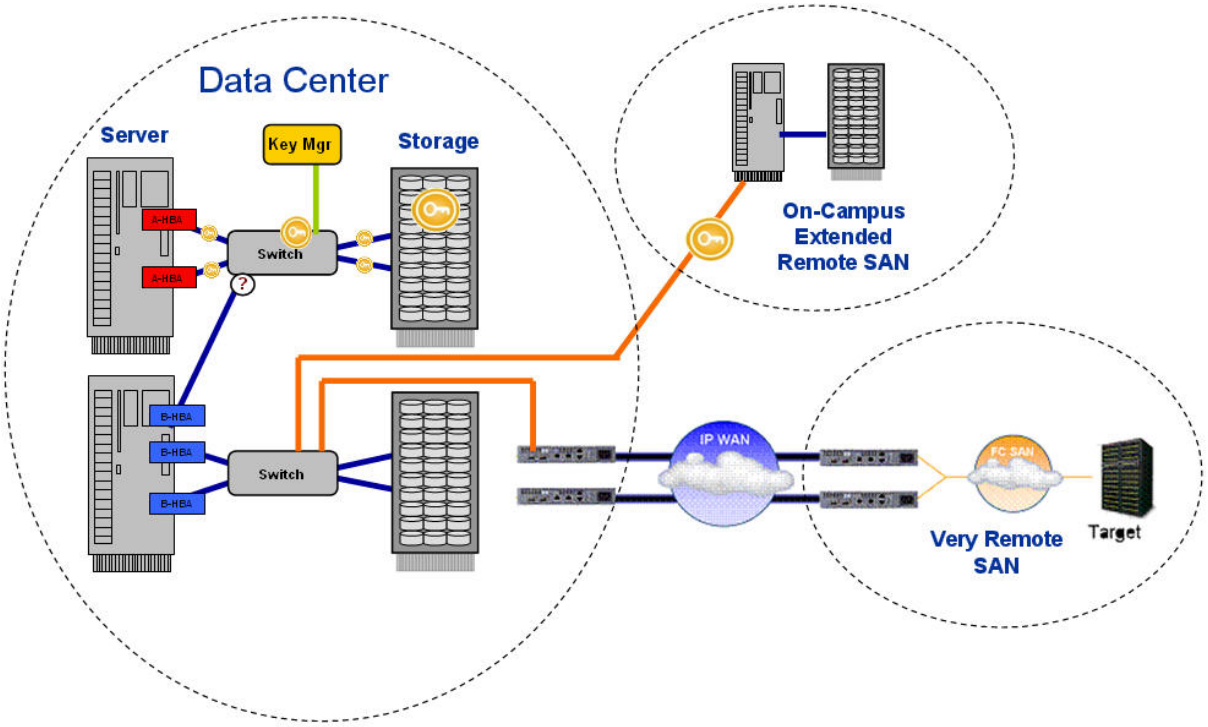


Figure 3. Overview of Security Approaches in and Across SANs

It may seem that encrypting in the fabric to secure the data on the hard drive is a good long term solution: the data is encrypted not only on the hard drive, but also as it travels through the fabric. However, rather than increasing security, this method actually decreases security by exposing encryption keys that are rarely changed (long-lived).

There are major challenges to hardware encryption at the switch or on the adapter. The farther away the encryption key moves from the data, the more complex the solution becomes. The more complex the encryption, the greater chance of error. For example, the right key may not be available to decrypt data when the time comes. This scenario is best explained via virtualization: the more equipment that is shared means that more entities must share a given key. Therefore, more keys are moving around in the fabric, and they are more difficult to track. The increased number of keys presents greater exposure, complexities, and performance issues.

The vast majority of data moving over the wire downstream of the file system is physically under the owner's control, and therefore is not considered a security risk. With physical security protection for the fabric, there is still the need to secure the data in the disk subsystem (i.e. on the hard drive) for when the drive leaves the owner's control.

For adapters with on-board encryption ASICs, there are interoperability challenges with multi-vendor adapters that do not support on-board encryption. Data encrypted by hardware on adapters can be read only by the same vendor's adapter or the proprietary solutions that created them. For instance, in Figure 3, the blue adapter cannot read data that is encrypted on the target or authenticate with the key manager or encryption switch. Every key manager handles keys differently, making interoperability a challenge. Non-encrypting adapters need special modified administration software to authenticate with key management systems.

Other storage system applications impacted by fabric encryption are data compression and de-duplication. These two applications can cut storage costs dramatically, but only when the data is not encrypted. Hardware encryption at the adapter or the switch level makes compression and deduplication very difficult or nearly impossible. This type of encryption is not only unnecessary, it can hurt interoperability in a multi-vendor environment.

There are significant implications to key management with different vendor's storage subsystems that use RAID controller encryption. Not all key management systems are the same. Even though they may use the same encryption algorithms, there are interoperability challenges between key management systems. Certain encrypted drive subsystems only work with specific key management systems.

SED DATA-AT-REST ENCRYPTION: OPTIMAL SOLUTION

Before Cavium started working on security in the SAN, the United States National Security Agency (NSA) addressed the problem of data security and determined that the best place to perform encryption is in the hard drive, because that's where the data resides.

Self-Encrypting Drives (SEDs) perform full disk encryption. During a write operation, clear text enters the drive and, before being written to the disk, is encrypted using an encryption key embedded within the drive. During a read operation, the encrypted data on the disk is decrypted before leaving the drive. The drive requires an authentication key (otherwise known as a password) from an outside source before the drive will unlock for read/write operations.

After authentication is completed during power-up, encryption is transparent to the storage system, which performs its traditional functions normally. Storage systems are optimized for unencrypted data for data compression and de-duplication.

Self-encrypting drives, when used with physical security for SAN arrays, address all the major security risks to data that exist downstream of the file system.

Key management is simplified in storage subsystems that use SEDs because the encryption key does not leave the drive. There is no need to track or manage the encryption key. The data center administrator does not need to store the encryption key to maintain data recoverability, because the drive keeps encrypted copies of the encryption key in multiple locations.

Given that SEDs decrease drive retirement costs with little impact to IT, corporations may benefit by incorporating SEDs into their security policy such that all future hard drive purchases are SEDs when available. IBM® and LSI Logic® are leading the way building SEDs into solutions. Seagate® is rapidly introducing SEDs across its entire portfolio of hard drives, and hard drive vendors world wide (Fujitsu®, Hitachi®, Samsung, Seagate, Toshiba, and Western Digitial®) are participating in the standardization of SED management, promising an end to the risk to data breaches when hard drives leave their owner's control.

In addition, it is easy to add disk drives with different embedded encryption algorithms to an existing array. The data center can have a mix of encryption algorithms in the same array, because the encryption algorithm is transparent to the system. As drive models change and new encryption technology is incorporated into hard drives, they can be intermixed with older drives in storage systems that support encryption without making any changes specific to the new drives' higher level of protection.

SUMMARY AND CONCLUSION

Administrators of servers and SAN arrays have good reason to want to encrypt data-at-rest. This paper addresses the reasons and the concerns that have prevented wide use of data encryption until now. There isn't a single comprehensive security approach or a single security technology that secures data-at-rest. Data encryption options include host-based software; encryption hardware appliances; and encryption ASICs that reside on adapters, switches, RAID controllers, and hard drives. There are costs, interoperability, performance, and latency issues that must be considered for each option.

Encryption in the hard drive provides simplicity, performance, manageability, and security relative to other encrypting technologies. For that reason, many analysts, system manufacturers, and government agencies like NSA are recommending that encryption for data-at-rest should be done in the hard drive.

ABOUT CAVIUM

Cavium, Inc. (NASDAQ: CAVM), offers a broad portfolio of infrastructure solutions for compute, security, storage, switching, connectivity and baseband processing. Cavium's highly integrated multi-core SoC products deliver software compatible solutions across low to high performance points enabling secure and intelligent functionality in Enterprise, Data Center and Service Provider Equipment. Cavium processors and solutions are supported by an extensive ecosystem of operating systems, tools, application stacks, hardware reference designs and other products. Cavium is headquartered in San Jose, CA with design centers in California, Massachusetts, India, Israel, China and Taiwan.

CAVIUM™

Follow us:

Corporate Headquarters Cavium, Inc. 2315 N. First Street San Jose, CA 95131 408-943-7100

International Offices UK | Ireland | Germany | France | India | Japan | China | Hong Kong | Singapore | Taiwan | Israel

Copyright © 2012 - 2017 Cavium, Inc. All rights reserved worldwide. QLogic LLC (formerly QLogic Corporation) is a wholly owned subsidiary of Cavium, Inc. Cavium, QLogic, and QConvergeConsole are registered trademarks or trademarks of Cavium Inc., registered in the United States and other countries. All other brand and product names are registered trademarks or trademarks of their respective owners.

This document is provided for informational purposes only and may contain errors. Cavium reserves the right, without notice, to make changes to this document or in product design or specifications. Cavium disclaims any warranty of any kind, expressed or implied, and does not guarantee that any results or performance described in the document will be achieved by you. All statements regarding Cavium's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.