

W
H
I
T
E
P
A
P
E
R

**DATA STORAGE
PROTECTION
*RISKS & RETURNS***

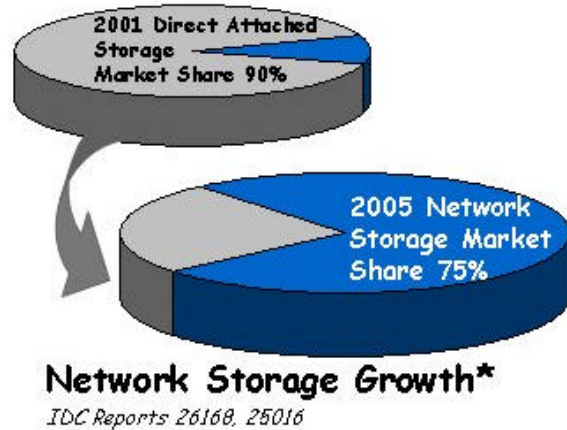


October 2002

INTRODUCTION

IDC and other research firms maintain that the majority of enterprise storage will be networked and distributed over the next few years – less than 30% of storage in 2006 will be direct attached. This evolution is driven by the demand for storage capacity, application availability and business continuity.

Regardless of the underlying storage connectivity, whether it is based on Fibre Channel Protocol (FCP), iSCSI (Internet Small Computer System Interface), or file-based network protocols (e.g., Networked Attached Storage, NAS), storage implementers must tackle known security challenges that threaten data integrity, accessibility and confidentiality. In doing so, enterprises may achieve reduced storage-management costs, greater storage utilization and increased data access.



Since greater availability means risk - what are the storage security threats and issues? What storage security countermeasures exist? How can data storage be protected? What is a Storage Security Appliance? What security considerations address which storage applications? And how can data storage protection be a cost-effective network storage enabler?

This paper explores storage network security risks, data storage protection and the advantages a storage security appliance can provide to augment distributed storage infrastructures.

Storage Security Challenge

The often quoted Computer Security Institute corporate computer security report conducted with support from the US FBI confirms an increase in overall information security breaches, with an aggregate financial loss in excess of \$455 Million in 2002¹. The most serious financial losses resulted from data theft. However, most companies still do not report security incidents, and almost all companies that participated in the survey are using traditional network and Internet access controls and defenses. The costs may be even higher if total downtime and response efforts associated with such breaches are figured into the equation.

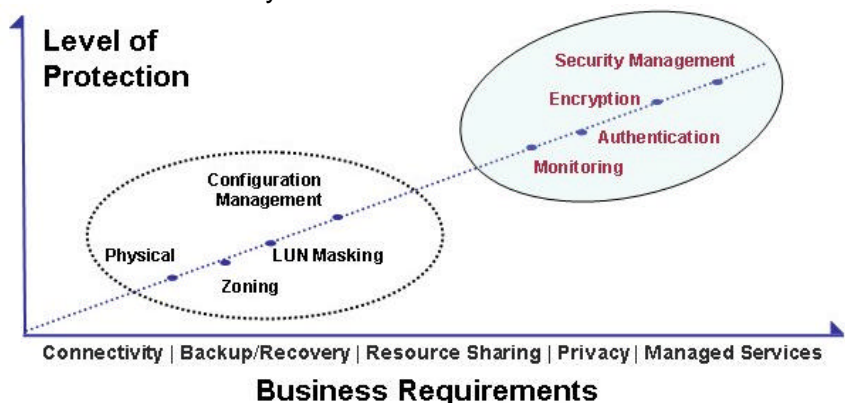
There is good reason to believe that networked storage resources represent prime targets - given the importance and centralized nature of corporate data. Storage networks, as with IP networks, are susceptible to published security threats such as system breach, spoofing, denial of service, unauthorized access, internal attack, data theft and corruption. Threat zones includes: systems / connections, storage fabric and management services, subsystems / media, and personnel with direct or indirect access to such storage components. Many such threats are being explored and are in varying stages of being addressed by a variety of industry consortiums and standards bodies including the Storage Network Industry Association (SNIA²), Internet Engineering Task Force (IETF³) and the International Committee for Information Technology Standards (INCITS) Technical Committee T11 for device-level interfaces⁴.

Since storage security often comes with costs and impacts, tradeoffs will be weighed against business requirements. Security costs can be measured in product capital expenditures, as well as deployment, management and maintenance. Losses are associated with data corruption, suspension of operations, and theft. For example, corrupted data can seriously affect a company's ability to conduct business and can affect operations. Breached / abused storage resources can materially affect operations. Stolen data can compromise a company's intellectual property, strategies and competitive advantage. In analyzing and establishing where and how to implement security practices, organizations must monitor, review and update their production and security policies – assuming they have any at all. Operational storage policies should be based on a risk assessment by storage function and business necessity.

Since no single security system is a silver bullet, a multi-tier defense strategy is a proven way to reduce risks.

Countermeasures for storage would include: system and device configuration, testing, auditing and monitoring, access authentication, logical unit number (LUN) masking, port zoning, and physical access controls. As companies

embrace more complex storage models, such as remote backup, disaster recovery, peer production sites, resource pooling, and managed services, additional layers of data storage protection will be required to defend a more distributed infrastructure. This will require data storage protection during transport, on the storage subsystem, and on the media.



¹ <http://www.gocsi.com/press/20020407.html>

² <http://www.snia.org> ; see the menu item for the Security Work Group

³ <http://www.ietf.org>

⁴ <http://www.t11.org/top.html>

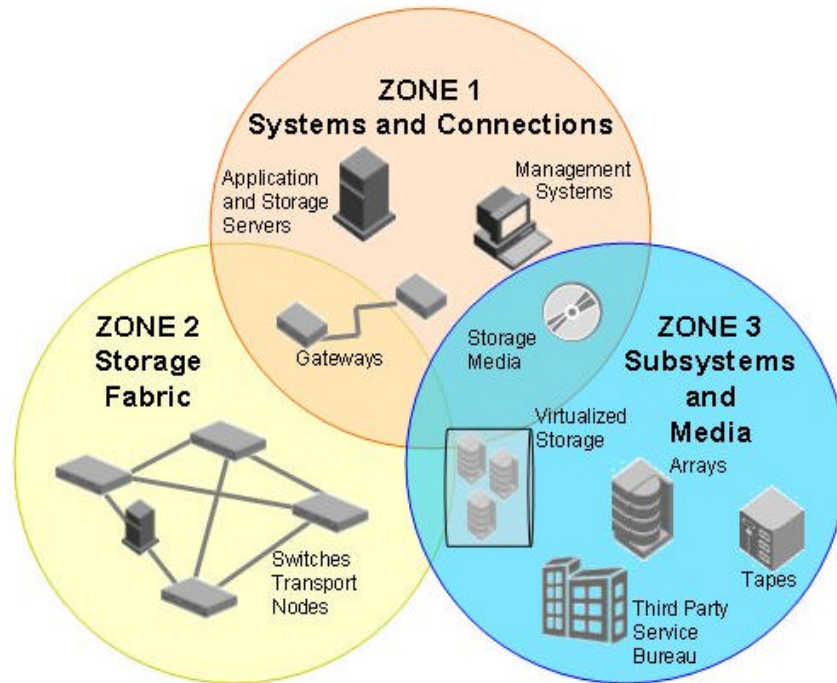
SAN THREAT ZONES

There are three threat zones that affect networked storage – regardless of the network protocol employed. These threat zones are systems / connections, storage fabric and management services, and subsystems / media.

SYSTEM / CONNECTION

The system / connection threat zone includes computer systems (such as application and management servers) and gateway devices that connect to storage infrastructures. Should

administrative or application access to the system or device be compromised / abused, the storage network may be vulnerable to unauthorized data access, denial-of-service attack and service loss. Unauthorized systems access is often obtained through poorly managed configurations, unused services or default settings. Once compromised, these systems can attempt to compromise media servers or issue abusive requests to storage subsystems for the purposes of data theft, corruption or service denial. IP and Fibre Channel (FC) defenses to thwart system breach include application / device access control, configuration policy assessment and system / device monitoring. However, it is possible to introduce a new IP or FC attached system due to weak auditing or just newly emerging SAN protocols which support authenticated storage access device provisions.



Fibre Channel storage area networks are associated with relatively short distances and restricted physical access. However, consideration should be made for protecting connected storage resources, shared storage and data leaving the data center (discussed later). To extend the SAN, gateways provide remote backup, replication and disaster recovery applications using dedicated, shared or public connections. Consideration should be made to the physical transport which may be susceptible to wire-tapping (certainly difficult, but possible), traffic interception / re-direction, gateway attack, etc. For example, without some degree of transport protection, frame or packet-based switching / routing networks can often be identified via ping sweeps and port scans. As such, enterprises are adopting company-leased or owned dark fibre⁵ to gain greater physical protection of their data.

Almost all storage components support out-of-band management, thus adding a layer of access. New IP and iSCSI devices also offer more ways to enter the storage network. Poorly configured access and management controls are often vulnerabilities allowing compromise of devices. For example, default device settings or open management ports can be easy pickings for attackers.

⁵ Dark fiber is optical fiber that spans some geographic area and is sold to carriers and large businesses without any optical or electronic signaling in its path. The customer is responsible for adding the transmission system at both ends. (See *Computer Desktop Encyclopedia*, <http://www.computerlanguage.com>)

Exploiting these vulnerabilities, it is possible to spoof FC or IP connections to capture, disrupt or redirect stored data / processes.

At present, pure FCP data transmission does not support native tunneling or virtual private network (VPN) services. Therefore, FC resident data and routing information are exposed. Until IP security (IPsec⁶) standards are adopted within FCP, the alternative method is to employ virtual private networking encryption services in conjunction with storage gateways that convert FC Protocols to IP. This protects data and routing information between IP-based SAN gateway connections.

STORAGE FABRIC

The second SAN threat zone is that of the storage fabric. Note that the fabric, while usually associated with Fibre Channel, in this discussion will consist of the hubs, routers, switches and applications that connect and manage data storage from data sources to disk / tape storage arrays regardless of transport protocol. As with most storage devices, vendors have implemented secure access capabilities to reduce the threat of device or management application hi-jacking – usually in the form of Telnet using SSH or Web using SSL for a secure connection. This is especially important for SAN applications such as port zoning, LUN masking and virtualization. Since most of these devices and applications support remote management capabilities, physical security will not defend against remote, out-of-band attacks. Should the switch, management server or management application be breached, the attack could result in material compromise of the storage network and pose a serious threat of data corruption. Even with strong access control policies, it is possible that a misconfigured or newly initialized storage device could lead to service interruption and data loss / corruption.

Today, the threat of unauthorized devices being attached to the fabric is relative to how closed the environment is to physical access and how often the fabric / network is audited. One example could be a rogue storage network attached server – a system with a FC HBA (host bus adapter) connecting to the fabric using a hi-jacked WWN (world wide name). Since there is no widely deployed authentication protocol between HBA, switch, and other devices on the FC network, this vulnerability is possible. A similar IP storage example occurs when a server with a network adapter attaches to a storage segregated network by spoofing an authenticated IP address. In both cases, data being transported may be visible to the attached node within the storage fabric. This presents data theft, corruption and denial of service vulnerabilities.

There has been recent activity to thwart the entity authentication vulnerability within the FC SAN community through the T-11 technical committee. ESP (Encapsulating Security Payload) has been specified for secure transmissions between SAN devices and it is widely used in the IP world and is also proposed for iSCSI through the IETF (RFC 2406⁷). It provides message authentication and optional encryption using keys (as described further). Although vendors are just beginning to implement ESP, the future looks brighter for fabric entity authentication.

To minimize this risk, storage administrators can implement zoning measures which would direct specific storage traffic through segregated switch ports – essentially configuring which storage sources and destinations can communicate. Soft zoning is accomplished through a switch's name server service by specifying nodes permitted to talk within a zone(s) by way of port number and / or World Wide Name. Hard zoning is enforced by inspecting the FC frame header and allowing pass-through traffic within a permitted zone(s) by way of port number or World Wide Name. Note that older switches, which are the installed majority, mainly supported hard zoning based on ports. Port-based zoning will rely on adequate physical security of the cabling. Soft zoning may allow a node

⁶ <http://www.ietf.org/html.charters/ipsec-charter.html>

⁷ <http://www.ietf.org/rfc/rfc2406.txt>

to directly talk to a target bypassing the name server. This is a similar approach in IP using router ACLs and stateful Firewalls.

Ultimately with zoning, only storage data and visible resources within the zone are susceptible to being captured, corrupted or abused. Network system scanners can possibly identify rogue, or mis-configured storage-attached systems.

SUBSYSTEM / MEDIA

The third SAN threat zone is storage devices, subsystems and media. This threat to “data at rest” is often viewed as a more serious risk than access to data in transit – as the potential exposure is more permanent. Unless encrypted by an application, stored data remains vulnerable. In many cases, applications are implemented with client to server data protection / encryption, but not server to backend storage. Beyond physical access controls and auditing, storage subsystem LUN (Logical Unit Number) addresses can be masked to further limit storage data visibility. The masking process is used to map LUNs that can be accessed only by specific hosts – essentially a host-based view of the storage resources. Hosts will not be able to request source resources that it can not “see”. This can be implemented via LUN masking services available on array controllers, switches, routers, device drivers and HBAs through vendor-specific or general purpose storage management software.

Tape media is considered the most reliable and most prevalent source for enterprise data recovery - whether used for remote / tiered backup, centralized secondary storage, or bulk data transport to service bureaus. While enterprises have implemented access controls and tighter infrastructure management provisions, such safeguards fall short of protecting the tape media itself

Portable storage media, such as tapes and optical disks, present an easy target for data theft. Unfortunately, most stored data on tapes are left in-the-clear on removable media which can be lost, stolen or compromised. Unauthorized users can readily read tape data, analyze confidential information, and in some cases re-build entire systems. Given that the data is removable, the perpetrators have more time and resources for tape inspection. In addition, failed disks with recoverable data may be sent to outside repair facilities where data may easily be copied. Misplaced and scratch tapes can be accessed. This requires secure media handling, disposal and auditing.

Virtualized tape systems are gaining visibility due to the advantages of restoration speed and ease of management. Here too securing data protection and access to said virtualized systems needs to be addressed.

OTHER SECURITY CONSIDERATIONS

Privacy

In addition to general security practices, many organizations must further assure the *privacy* of their data. Sweeping legislative changes in financial, healthcare and commerce have created liabilities for enterprises that fail to ensure data privacy at all data access points including storage. Such compliance includes the United States legislation known as HIPAA⁸ and GLBA⁹ as well as directives from the US and European Union (EC Data Privacy Directive¹⁰).

⁸ Health Insurance Portability and Accountability Act, <http://www.hcfa.gov/medicaid/hipaa/default.asp> ; see also http://www.aha.org/hipaa/hipaa_home.asp

Continuity

To alleviate business continuity threats, organizations are developing remote storage capabilities. Depending on the storage function, this may include remote backup, tape vaulting, storage-array mirroring, peer operation sites, and the use of storage-service providers. This strategy significantly reduces the threat to operations due to physical disaster, application or system outages, and human error; however, it can also increase the number of people and entry points with access to storage resources and data.

Consolidation

Many storage resources, including most deployments of networked storage, are managed as silos - tied to distinct applications or business units. This has occurred as a means of assuring confidence to the owner (e.g. department x) that their data was accessible, protected and directly controlled. Companies are now attempting to consolidate storage systems in order to maximize / virtualize capacity and minimize management overhead. Should departments or subsidiaries have sensitive or regulated data, added data access safeguards may be required to support consolidation efforts.

Management

Storage administrators and service providers who manage and support storage processes / resources have access to this data. For example, system backup tapes which are small, portable and typically stored outside confines of the data center for off-site disaster recovery. Again, since internal and other support staff may have greater physical access and are typically more knowledgeable about system configurations and data locations, minimizing access abuse must be considered. Managing discrete access controls and security procedures for managing all storage-related applications, systems, devices, and media reduces this risk.

In short, data encryption and access controls at the application, system, transport and media levels can provide strong barriers against unauthorized stored data disclosure, theft and corruption – and can alleviate privacy requirements for storage extension and consolidation. It complements a layered approach to securing storage infrastructures.

⁹ Financial Services Modernization Act, generally known as the Gramm-Leach-Bliley Act,

<http://www.senate.gov/~banking/conf/grmleach.htm> ; see also http://www.gibsondunn.com/publications/Uploads/gdi_glb.asp

¹⁰ European Union “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,” http://www.cdt.org/privacy/eudirective/EU_Directive_.html

DATA STORAGE PROTECTION

Methods for protecting stored data within both direct attached and network storage infrastructures have historically been non-existent, but are improving. As mentioned above, switches, hubs and routers already support authenticated access and the ability to apply port segmentation and zoning. Most storage subsystems and storage-management applications support LUN masking. IP storage can support VPNs for data transport protection. And, vendors within the FC community are advancing their FC switch-to-switch authentication methods.

Storage fabric entity authentication will play a critical part in reducing unauthorized access risk... further enhancing availability, integrity and confidentiality. As mentioned above, the T11 committee has proposed that storage devices employ ESP for authenticated communications. This will require key management which includes session key lifetimes (how much data and packets transfers are allowed before a new key is required). T11's FCSP committee recently settled on DH-CHAP (Diffie-Hellman Challenge Handshake Authentication Protocol) for entity authentication DH-CGAP employs a shared password based scheme with administration offloaded to a centralized RADIUS type service. In addition, vendors can also incorporate digital certificate based authentication schemes. Again, these advances cover how devices will be allowed to attach and communicate in the fabric.

In addition, the IETF is proposing IPsec protocols to be implemented within both FC and iSCSI SAN solutions for data transport tunneling and authentication; IPsec will also require an additional layer of integrated storage-security management. As demonstrated by current IPsec VPNs, vendor adherence to IPsec implementation standards can and will vary. Corporate SAN architecture, growth strategy and business requirements will ultimately dictate whether such tunneling capability should be implemented at switch level, system level (e.g. host bus adapters) or through gateway devices (similar to that of IP networks).

Tunneling protects data only while it is in transit between two tunneling devices. Encrypting stored data extends protection all the way to the physical media. A user or system can read encrypted data only if decrypted by the originating application's authentication method, using encrypt / decryption key(s). Storage vendors are looking at cost effective means to deliver data privacy within a distributed storage infrastructure without impacting performance or increasing complexity. Considerations for implementing data storage encryption include media type, strength, key manageability, performance, reliability, cost and application.

Data encryption on storage media requires special consideration of compression, key management, data recovery and strength. Writing data to tape does not impose fixed block sizes and is thus readily compatible with data compression, authentication and encryption techniques. For recovery purposes, encrypted tapes may need to contain metadata that securely reference the encryption system used to protect the tape. This security metadata is especially important if that stored data is maintained for a long time, such as when data archives are mandated (e.g., by HIPAA). However, writing encrypted data to disk media may have additional restrictions which are imposed due to fixed block size. For disks, automated key management and authentication may need to be addressed outside the disk media. In most cases, authentication can be handled directly or by encrypting the application-provided checksums that accompany the stored data. This approach complements and does not duplicate the authentication and integrity checks already supplied by most applications.

In terms of encryption, one should also consider the algorithm employed in terms of strength. For example, Data Encryption Standard (DES) key lengths of 56 bits are now considered weak because brute-force testing of the entire keyspace is relatively quick and inexpensive using easily available processing capacity. 3DES is considered more credible because its effective key length is 112 bits,

requiring much more time and processing power to crack a key (3DES requires 2^{56} or $>10^{16}$ more effort to break than DES). More recently, the U.S. government supported the AES (Advanced Encryption Standard) algorithm which employs 128-bit / 256-bit block data encryption. Another outcome of encryption may include data integrity and authentication – preventing tampering or repudiation. They also will define how keys are selected or qualified, implemented and maintained.

IMPLEMENTING DATA ENCRYPTION

Depending on the storage function, the level of data protection required and the trust zones along the storage path, data encryption can be implemented at several levels which include:

- at the application level
- as a component of a storage application (e.g. backup or replication)
- as part of the fabric switches
- and now as an in-line storage security appliance

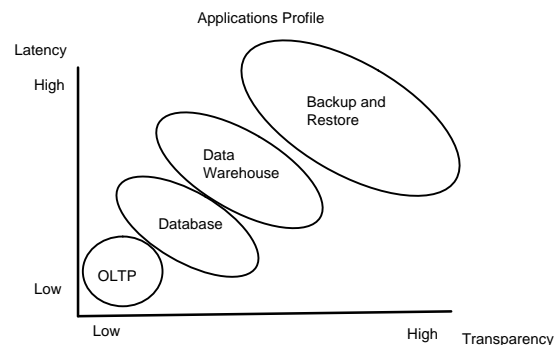
Employing encryption at the application level introduces the challenge of coordinating different protection schemes which can complicate data recovery and restoration. Application data protection is usually implemented between the client and the server but does not often extend to the storage subsystem. Additional application-level encryption to the storage array may require modifying the file system, database system or the application itself. In many cases, retrofitting existing applications for such encryption can be very difficult and expensive.

Encryption keys are used for proper and secure identification among entities involved in data exchange, as well as a means to encrypt and decrypt the data itself. Part of the difficulty with implementing encryption at the file system or storage application level is how encryption keys are exchanged, stored, authenticated and updated. Automated key exchange can be used to establish a temporary tunnel between two storage devices. With media data protection, keys will need a longer life – and may be susceptible (1) to being abused if the host system they reside on is compromised or (2) to being breached using brute force attack. Due to this risk, encryption keys should be protected against theft. For example, some backup applications place the encryption key on each host system and employ relatively weak single 56 bit DES.

As mentioned prior, switch vendors have started to provide strong switch-to-switch authentication and there is adequate movement in the storage industry to support SAN entity authentication. This authentication adequately assures that a device connecting to the fabric is authentic and allowed. However, this approach does not protect the stored data in transit or when they reach the subsystem or library. Implementing data encryption at the switch or even at the subsystem level requires additional performance, key exchange methodology, interoperability and security management capability.

One consideration for the customer is the degree of latency acceptable by the user in terms of the impact on the company's storage function / application. Latency relates to the period of time between element interaction within a defined system. More specifically, how much processing is required to execute a security policy between storage source and destination? The greater the latency, the greater the impact on storage services and the greater the possibility that other components used within a storage function will be negatively affected.

In most cases, implementation of data storage encryption will not be a SAN or NAS issue, but more importantly, a determination of security importance between primary and secondary storage. Ideally, the best solution provides the lowest amount of latency and the greatest transparency in operation.



The most fundamental consideration will be the cost of implementation for the customer. Placing encryption at the application, file system or storage application levels places an enormous processing burden on the host system and degrades response time. If enhanced data protection requires upgrading or replacing servers, switches, routers and arrays, then such defenses may be too costly - the protection could indeed cost more than the data or function being protected. These approaches may also require storage architecture changes that would further add to deployment costs.

STORAGE SECURITY APPLIANCE

A storage security appliance has the advantage of high performance, centralized, policy-based management and transparent operation. The appliance analyzes stored data traffic, dynamically applying appropriate encryption and forwarding the encrypted payload to the storage subsystem without impacting the surrounding storage operations. By placing the encryption functionality and processing in a built-for-purpose device, the server or application storage processing remains dedicated.

Alternatives	Performance	Manageability	Cost	Deployment	Security
Application / File System	Server Impact / App Response	Difficult: New Schema Per App / OS	High	Difficult: Per App	Strong Per App
Storage Management SW	Server Impact	Difficult: too many keys	Med	Difficult: Per System	Strength Varies
Fibre Channel or iSCSI Switch/Router	Network Impact	Varies by Vendor	High	By Device... May Require Replacement	Varying Stages
Storage Security Appliance	Bump in Wire	Convenient	Low	Immediate	Strong

Data encryption within a storage appliance can be implemented in several ways. The first method is broad application using a single or reduced key set. A single set of encryption keys may be employed for all data entering the appliance. This would minimize the manageability of keys but will still require key escrow and a mechanism to tie an encryption key to a block range, partition, tape, object, etc. However, this approach does not take into account unique applications or protecting different sensitive data with different keys. Many companies would prefer to selectively encrypt sensitive stored data and leave non-confidential data alone. By not associating unique keys with unique data storage applications (e.g. by department, subsidiary, customer, data type, application type), those with access to the single key could have access to the kingdom. Given the risks and manageability defects, broadly applying data storage encryption with a limited key set has limited capability.

The second method is to provide dynamic and automated data storage encryption based on user-defined rules. This approach allows data encryption to be applied in response to different business requirements. Rules would be created by the user and maintained by the appliance. Each rule would comprise data storage protection parameters based on selectable data elements that would be available as part of the knowledge-base of the storage security appliance. For example, rules could be based on source or destination including support for Zones, LUNs, ports and worldwide names. Application level support, such as the support for volumes, block ranges and unique frame payloads, may require more robust application knowledge and integration. This approach takes into account how organizations protect different application or functional data storage.

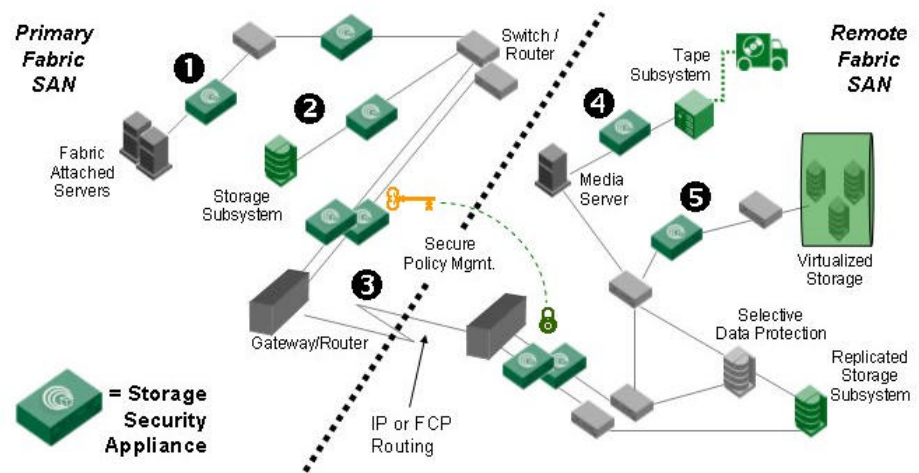
Performance is a significant consideration as it may affect surrounding processes. As storage data enters the storage security appliance, data is encrypted and then forwarded. Performance is affected by the encryption algorithm, and the level of detail and speed at which storage data could be processed. Performance requirements will vary by data storage application and connection distance with regards to backup, mirroring, and transactional storage. However, encryption processing capacity, be it multi-gigabit or sub-gigabit, alone is only one consideration. As mentioned above latency will be critical for high-transaction oriented storage applications.

A storage-security appliance can centralize and automate key management. For protection, the system itself must employ effective system hardening, authenticated access and master-key protection. An appliance should support different means to incorporate keys; such as manual, through key servers, and self-generated. These keys can be associated with rules for both transport and media protection. Since the keys are maintained in the appliance rather than

distributed on multiple systems, the storage data protection processes can be managed effectively, centrally – and securely. Essentially, the encryption keys used to encrypt the data should themselves be encrypted and never leave the appliance ‘in the clear’. The keys should support user provided keys and true random number system generated keys – common to most encryption devices.

A storage-security appliance operates in-line and can be transparent to the application, to the storage subsystem, and can even be transparent to the switch or router. An appliance can be deployed according to an organization’s security requirements such as:

- (1) between application-attached storage servers and the fabric,
- (2) within the fabric,
- (3) before or after gateway connections,
- (4) in-front of storage subsystems and
- (5) in front of virtualization systems.



Once stored data reaches the appliance, the data payload can be encrypted and sent forward or through a secure tunnel (in which the appliance or another device is the terminating point). If tunneling functionality is employed, the appliance will require awareness of switches or routers. This flexible deployment can effectively complement security provisions such as port zoning. For example, the appliance can be associated with zoned ports that carry application-specific or sensitive storage data. Such a deployment can also adapt to current and evolving network storage topologies and business functions.

Lastly, a storage security appliance must offer exception enterprise manageability, interoperability and reliability. Since storage resource management may be distributed, the system should support secure remote configuration, maintenance and updating. Since storage systems and connections are often redundant, so too should the storage security appliance support redundant deployment. Reliable operation and failover capability will ensure that when a line or system failure occurs (even in disaster situations), the re-routed storage traffic will be treated with the same storage-security policy. For recovery purposes, the appliance should allow for a secure means to export the encryption rules and associate keys with storage data. Therefore, if the appliance needs to be restored or the data needs to be retrieved in an emergency, the respective data can be readily obtained.

DATA STORAGE PROTECTION BENEFITS

Data storage protection can be applied to risk reduction efforts, as well as fostering greater SAN growth and adoption alternatives. NeoScale is pioneering the use of data protection within distributed storage infrastructures with the introduction of a dedicated storage security appliance - NeoScale CryptoStor™. CryptoStor offers wire-speed performance, centralized management, flexible deployment, policy-based data protection and access control, standards-based block-level encryption, automated key management, failover redundancy, SAN interoperability, and secure data preparation / recovery options. The following are applications that can be addressed by an enterprise storage security appliance.

Removing access and theft risks associated with data storage leaving the data center

Many organizations rely on internal physical and access controls to protect their storage resources and data. However, this level of protection may not exist or may not be as strong once data has left the data center. Data storage protection during transport and on the media addresses this risk.

Enforcing privacy compliance to arrays and tapes containing sensitive / regulated data

Stored data may contain company sensitive or government regulated data. While government legislation such as HIPAA, GLBA, FDA and EC Directives require that data be protected from unauthorized access, compliance does not necessarily dictate encryption. However, encrypting stored data does demonstrate due diligence and makes accessing data without authorization a significant challenge.

Maximizing resource utilization through protected storage pools and virtualization

Many corporate departments and subsidiaries maintain their own 'protected silos'. In some cases, these silos are kept so as to assure accessibility and to protect sensitive data. For example, the engineering department may have sensitive research data which are to be segregated and protected from the human resources department; conversely, the HR department may have sensitive personnel data which should be segregated and protected from the customer services department. However, this silo approach can introduce inefficiencies related to separate storage resources and added management costs. By encrypting stored data with keys for unique functions, applications or departments, it is possible to securely pool storage resources and keep costs down.

Enabling alternative storage capacity and business continuity options

As mentioned earlier, rarely do organizations have a surplus of storage resources and funds to address their burgeoning primary, secondary and distributed storage demands. It is difficult to anticipate material capital expenditure associated with different storage requirements. Sometimes, data storage needs exceed available storage capacity. It may be necessary, by business function or as a stop-gap measure, to seek alternative or temporary storage capacity within and outside the organization. Similarly, business continuity may require the use of external data storage facilities. Encrypting stored data can further assure that data being stored in alternative repositories are protected.

Advancing application data protection beyond client / server to storage media

Application-layer data encryption is an effective way to ensure data storage protection and integrity. In many cases, the data protection lies in client-to-server secure communications. Adding data protection from server to storage array can be costly in terms of after-the-fact engineering and the additional processing load required for encryption. It also can require coordinating different protection schemes that may not fully adapt to storage infrastructures. Encrypting data using a storage security appliance can address both performance and management complexity issues.

Enhancing actual and perceived trust with internal / outsourced managed storage

Internal IT storage resources or managed service providers must not only demonstrate an ability to meet storage capacity, accessibility and resumption service levels, but also the security measures that segregate and protect client data. Adding data storage protection can address this issue by enhancing both the actual and perceived data handling safeguards. This allows the internal or external managed storage provider to focus on administering the data, while relegating key and security management to the client.

Eliminating unauthorized or incidental data access on failed disks and exported tapes

By encrypting stored data on both disk and tape, organizations can potentially eliminate the possible unauthorized access to storage media. Furthermore, data storage protection can add greater security for businesses that employ service bureaus to process or store data send to them via tape.

Complementing security and business requirements without the costs associated with architecture re-engineering and infrastructure replacement.

As described earlier, a storage-security appliance centralizes the data storage protection policies and can be flexibly deployed within a variety of storage infrastructures. By not requiring organizations to replace storage resources or modify current architectures, a storage-security appliance can be a cost-effective way to meet current and evolving security and business requirements.

SUMMARY

Enterprise storage used to exist in a relatively fixed, centralized, controlled environment where physical security, access controls and known administrative entities satisfied requirements for management due diligence. In the wake of greater demand for storage capacity, application availability and business continuity, most enterprises will migrate to networked storage. As such, storage implementers must address known storage area network (SAN) security challenges in order to realize the benefits of greater resource utilization and data accessibility.

The most costly information technology security losses occur through theft of proprietary data, and backend storage resources represent prime targets. In addition, regulations governing finance, commerce, healthcare and government data use have created obligations to ensure data privacy at all storage levels.

No security system is a “silver bullet.” A tiered defense strategy incorporates system and device configuration, testing, auditing and monitoring, access authentication, LUN masking and port zoning, physical access controls, and data storage protection during transport, on the storage subsystem and on the media. To protect backend stored data, block-level data encryption can be employed to eliminate the risk of unauthorized access stored data “in flight” and “at rest.”

Storage security appliances can be a key part of a complete strategy, combining excellent storage protection with efficient network-based management, lowering the cost of enterprise storage protection. A storage security appliance provides wire-speed encryption, transparent operation and centralized, policy-based data storage protection. This appliance approach offers a cost effective, high performance means to deliver data privacy within a distributed storage infrastructure without degrading backup, replication, mirroring and other storage functions. It also offers significant benefits including:

- Removing risks of open access and theft related to stored data leaving the data center
- Enforcing privacy compliance for arrays and tapes containing sensitive / regulated data
- Maximizing resource utilization through protected storage pools and virtualization
- Enabling alternative storage capacity and business continuity options
- Advancing application data protection beyond client / server to storage media
- Enhancing actual and perceived trust with internal /outsourced managed storage
- Eliminating unauthorized or incidental data access on failed disks and exported tapes
- Complementing current security provisions and business requirements without the costs associated with architecture re-engineering and infrastructure replacement.

Greater data availability does require stronger controls to shield storage resources. Employing a multi-tier defense strategy is a proven approach to safeguard enterprise storage investments. A storage security appliance complements this defense strategy and fosters greater SAN expansion and resource utilization by cost-effectively providing strong, scalable and manageable data protection.

ABOUT NEOSCALE

NeoScale Systems, Inc. is a leading provider of enterprise-class security solutions for data storage. The company is bringing to market a suite of products designed to add scalable, high-performance, strong encryption and authentication services that enable organizations to readily achieve data storage confidentiality in a variety of online, nearline and offline storage environments. The resulting solution lowers the cost of protecting highly accessible, distributed storage infrastructures, while also enabling greater efficiencies for the management of storage capacity, consolidation, continuity and availability

NeoScale CryptoStor™ is a family of wire-speed, transparent, policy-based storage security appliances and related products that enable organizations to readily achieve storage data confidentiality - simply, reliably and securely. CryptoStor *FC* is the industry's first inline, high performance storage security appliance that offers transparent, policy-based storage data encryption, storage tunneling, storage firewall services at line rate for Fibre Channel SANs. CryptoStor *for Tape* is the first enterprise class data protection appliance for networked, remote and direct attached tape and virtualized tape systems.

For more information, please contact NeoScale at 408-586-1300 or visit <http://www.neoscale.com>

About the Author

Scott Gordon is NeoScale's Vice President of marketing, responsible for worldwide product, promotion, and sales support strategy. He has contributed articles, white papers, industry, and product development efforts on such areas as storage security, intrusion detection, security management, virus defense, security policy, and encryption. Scott holds a masters degree and earned his BBA degrees in Marketing and MIS from Hofstra University.



NeoScale Systems, Inc.
1500 McCandless Drive
Milpitas, CA 95035
408-586-1300