SNIA

Storage Security Industry Forum

Solutions Guide for Data-At-Rest

BROCADE

hp invent

IBM

NetApp

Seagate

THALES

wave

Table of Contents

Introduction

The SNIA Storage Security Industry Forum (SSIF) of the Storage Networking Industry Association (SNIA) has produced the **SSIF Solutions Guide for Data-At-Rest** to address some of the concerns that have arisen with the recent focus on data privacy, integrity, availability, and liability.

The purpose of this document is to provide guidance into some of the factors you should consider when evaluating storage security technology and solutions. As with any security project, acquiring technology is not the only step to properly protecting your data. Part of this process should include an evaluation of the current processes and security controls in place, such as physical access controls, environmental controls, and administrative controls. While there is no single set of requirements that applies to all organizations, this Guide can provide some baseline considerations.

This Guide provides an overview of solutions provided by our members to mitigate the threat of loss of physical control of storage media.

This Guide will first provide background information describing various storage security threats related to loss of physical control of storage media. With that foundation, we then review the various methods for mitigating these threats including both the scope of available solutions and the various implementation choices that exist.

Finally, there is a capabilities comparison matrix that compares and contrasts the available solutions accompanied by a vendor-supplied summary of each of the SSIF member's solutions to provide you with information to assist you in making a product decision. This information has been provided by the individual vendors and no independent verification of the claims has been made.

Why Should You Encrypt Your Data?

Data in networked storage environments is significantly more vulnerable to unauthorized access, theft, or misuse than data stored in more traditional, direct-attached storage. Aggregated storage is not designed to compartmentalize the data it contains, and data from different departments or divisions becomes co-mingled in the network.

Data backup, off-site mirroring, and other data replication techniques may increase the risk of unauthorized access from people both inside and outside the enterprise. Partner access through firewalls and other legitimate business needs can also create undesirable security risks, and current research indicates a significant percentage of attacks come from within the firewall. With storage networks, a single security breach can threaten the data assets of an entire organization.

Data in cleartext is vulnerable to attacks. Curious or malicious insiders, administrators, partners, hackers, contractors, or outsourced service providers can all gain access to data quite easily.

Technologies such as firewalls, Intrusion Prevention Systems (IPS), and Virtual Private Networks (VPN) seek to secure data assets by protecting the perimeter of the network. LUN Masking and Zoning in SAN environments also attempt to address concerns about security. Unfortunately, these targeted approaches do not adequately secure storage, as data is still stored in cleartext, dangerously open to a wide range of internal and external attacks.

Encrypting your data-at-rest on tape and disk will significantly mitigate these threats and allow you to secure your data while maintaining your current service levels for operations.

Threat Model for Data-at-Rest

In the larger picture of storage security there are a variety of threats to the networked storage systems such as:

- Compromise of systems with access to the data,
- Compromise of the networks attached to the storage systems,
- Compromise of the storage devices, and
- Loss of control of storage media.

Information security and data privacy require a number of security mechanisms beyond the threat of the loss of control of storage media. For instance, data is often replicated and if data can be copied from a secure system to an insecure or rogue system then that information is at risk or lost. Access control systems on servers, within applications, and implemented by file systems and filers provide a layer of security for limiting access to information based upon authentication of the user and the permissions set on the information access.

The *SNIA Technical Proposal Storage Security Best Current Practices (BCPs)* has a more comprehensive discussion of the threats and best practices for protecting your networked storage. The solutions described in this Guide complement but are not a substitute for implementing the best practices for storage security as outlined in the technical proposal. This Guide is restricted to the threats related to the loss of physical control of storage media.

Nearly all media eventually leaves the owner's control. The majority of media leaves the owner's control when it is decommissioned at its end of life, end of lease, or is returned for warranty or repair. Loss of physical control of storage media include media types such as:

- Removable media like tape cartridges ,
- Disk drives in servers,
- Disk drives in networked storage,
- Media in desktop PCs and workstations,
- Portable storage such as in laptops,
- Intermittently connected storage such as USB flash drives.

Even if the media is decommissioned due to failure, the data on that media may still be able to be read. The data that is on the vast majority of the hard drives, for example, even if it is a failed device, is still able to be read. Drives that were part of a striped array are also at risk. The typical stripe size in today's arrays is big enough to expose hundreds of names and social security numbers.

Some companies aim to put in place rigorous controls to require data cleansing prior to recycling the media. However, all of these security processes are dependent on human beings to not misplace or miss any media that needs to be sanitized before leaving the owner's control. And each of the processes is not foolproof.

Overwriting the media may take hours or days, miss re-allocated portions of the media, or not work at all under certain failure conditions, and there is no indication of when the process is complete.

Other processes (degaussing, physically shredding, or other physical destruction) often requires shipping the media to another site where the degauss or shredding equipment is located, exposing the media to the risk of transport of unsecured data. This physical destruction does not permit the media to be repurposed, or returned for expired lease, warranty or repair,

These data cleansing issues and the increasing risks of data exposure have increased the interest in encryption. Encryption can automatically secure the data when the media leaves the owner's control, without dependence on humans and costly, time-consuming, imperfect processes.

Storage Security Solutions

In general, protection of data when you have the risk of physical loss of control of the media involves the use of encryption. These solutions will include:

- Encryption/decryption process;
- Key management to protect and store encryption keys;
- Integration with the processes and systems accessing the data.

Classic tradeoffs of performance, complexity, and ease of use apply to the use of encryption and each solution has advantages and disadvantages that arise from those tradeoffs. As the storage security marketplace has evolved, and as customer requirements have increased for storage media data to be encrypted, vendors have been working to minimize the impact of introducing encryption - making it as simple, transparent, and cost-effective as possible.

Encryption Strength

As encryption algorithms age and processor power increases, today's algorithms will progressively become more vulnerable to breaking. Encryption algorithms such as DES, 3DES and hashing algorithms such as MD5 and SHA-1 are generally considered to no longer be secure. Solutions should take advantage of the strongest commercially available algorithms such as AES. It is also important to consider the end-to-end security of a system – encryption is only as strong as its weakest link. If you encrypt using AES-256, but store your keys in cleartext and leave them in an open operating system, it will be fairly easy to compromise the entire system. Because of the changing nature of encryption standards, it's also important that your encryption solution can be upgraded to address emerging standards, without requiring full hardware replacement.

Product Certifications

Solutions should have gone through formal, independent certification. The standard certification body for encryption technologies is the National Institute of Standards and Technology (NIST), who tests and certifies third-party products against a standard called the Federal Information Processing Standard (FIPS). Other certifications, most notably the international Common Criteria standard, are also used to validate that encryption products have been built properly. Without independent validation, it is difficult to ensure the products perform as promised. For security solutions, using encryption, this is even more critical.

Implementation Choices

Encryption

Choices for where and how to implement encryption have traditionally required trade-offs for performance, complexity, and ease of use. The processors in servers for instance may not have the spare CPU cycles to perform the cryptographic functions required without incurring a performance penalty for the application running on a server. Adding encryption may require you to change the application or require different user behavior. In the storage network there may be challenges with encrypted data as encrypted data does not lend itself to traditional compression and de-duplication techniques. Adding cryptographic functions may add additional cost to storage systems by requiring new processing capacity.   Obviously, users would like a solution which does not adversely impact performance, does not introduce management complexity, and does not introduce opportunities to lose access to their data, and can be monitored and audited.

Adding encryption also implies the need for key management that has its own set of challenges including:

- Loss of the key can result in loss of the data,
- Keys have to be kept secure but be available wherever the data is having cryptographic functions performed on it,
- Keys have to be retained as long as the data needs to be retained,
- Keys have a lifecycle including the need to be created, changed, and destroyed, and
- You would like to have the keys managed without introducing a lot of cost or operational complexity.

Encryption in the application

If you can identify specific data which you need to protect you may be able to encrypt just the sensitive or valuable data. For example, in a database application you could enable encryption at the column level. A common example of the use of this technique is to protect particular fields required by an industry standard like the Payment Card Industry Data Security Standard. The advantages for this type of approach are that the amount of data being encrypted is minimized so that the performance impact on the application is potentially minimized.

The challenges for this type of approach include the ability to properly identify all fields which contain sensitive or regulated data and ensure that any changes to the application or schema include the consideration of whether they should be encrypted. There may also be further challenges, as application encryption is also specific to a given application. If you have multiple applications that require access to encrypted data it will be difficult, if not impossible, to find compatible solutions that will utilize a common key management infrastructure. Further, it is likely that one or more of your applications will not natively support its own encryption mechanism.

Encryption in the file system or operating system

In a number of operating systems there are options for either turning on encryption in the native file system or adding an encryption facility on top of the native file system. Traditionally there may be additional software that is installed on a server and invoked by the user to encrypt/decrypt individual files. Performing selective encryption may reduce the impact on performance. In addition, as host processors in devices like laptops became more powerful, full disk or full file system encryption has been introduced. The advantages of using selective encryption by file is that it can reduce the performance impact but users may have to be involved in invoking the encryption and decryption as an extra step. By encrypting all files users may not see the encryption and decryption steps but there may be a performance impact.

Performing encryption in your servers can be a double-edged sword. It does allow you to provision your encryption processing where it is needed. The downside, however, is that it will likely be intrusive to the operations of that server. If encryption is done in software, performance on that server will be significantly impacted whenever a non-trivial amount of data needs to be encrypted. It may be possible for encryption is to be done in specialized hardware added to these hosts, however, there will be downtime for each server to be shutdown, have the coprocessor installed, reboot, install appropriate driver software (and perhaps reboot again), test your applications, and bring back on line. In large enterprises with tens, hundreds, or thousands of servers this could be extremely invasive to your operations. Further, as this deployment will not happen instantaneously, you will need to plan very carefully the rollout as there will be periods when some servers are encrypting data and others are unable to access it. Finally, it is important to find a solution that supports all the host configurations (both hardware and Operating System) that you have today and will use in the future. Again, in large and varied enterprises this could be a challenging task.

Encryption in the device driver or network interface

You can encrypt in the network interface such as a host bus adapter or network interface card. Some network cards now include dedicated hardware logic for accelerating the cryptographic functions. The information is protected from the server through the SAN to the storage. Currently, this type of solution tends to focus on data-in-flight versus data-at-rest where there is a possibility of capturing data in flight and performing an analysis to find the keys and access the data. Temporary keys are used and periodically updated. When solutions focus on data-at-rest encryption keys protect data for much longer periods of time. This requires that the length of the key and strength of encryption is sized appropriately and key management includes the ability to maintain keys for long periods of time.

Encryption on the network

Network-based encryption offers the key benefits of centralized encryption and key management and enabling encryption on existing storage devices. The centralized approach of encryption in the network uses one key vault and management application to encrypt data for multiple types of heterogeneous storage (disk and tape). Instead of buying several devices that enable encryption for a given application, network-based solutions encrypt data for multiple applications and use the same user interface to manage encryption policies. Network-based implementations enable encryption from a centralized location to existing storage devices.

Without upgrading end devices, network-based encryption can selectively encrypt data to meet the needs of the organization. For disk-based encryption, the user can configure encryption at the logical unit (LUN) level so only specific application data is encrypted on large storage arrays. For tape-based encryption, data encryption keys can be associated to individual tapes or tape pools to refine the granularity of encryption. While some initial deployments added significant latency to the encryption process, the latest generation of solutions adds less than a millisecond of delay to ensure backup windows are maintained in tape applications. With network-based encryption, users have the flexibility and power to encrypt data on legacy storage devices and encrypt only the data than needs to be encrypted.

Encryption in the storage controller

The storage controller can perform encryption in the logic between the network interface and the storage device. While the controller cost may increase by adding the cryptographic processing it may have the advantage of using non-encrypting capable devices.

Encryption in the storage device

Self-encrypting storage devices imbed encryption in the storage device itself, providing full disk encryption so that fine grained data classification is not needed and the device can leave the owner's control securely.   Self-encrypting devices are unique in that they do not expose the encrypted text which is an aid to an attacker. Neither the encryption key nor the encrypted text ever leave the device, enhancing security, greatly simplifying key management, and making the encryption transparent to the OS, databases and applications. Since the encryption key does not leave the device, there is no need to track or manage the encryption keys.

Cryptographic processing within the device can make no measurable performance impact to the system, and allows the encryption to scale linearly automatically as more storage is added to the system. All data can be encrypted, with no performance degradation, so there is no need to classify which data to encrypt.   It is easy to securely erase the entire device in less than a second by erasing the encryption key in the device, without worry that there may be a copy of that encryption key somewhere outside the device. Since the key has never left the device and there is no other copy, the proof of data destruction is the execution of that single task.   The need to re-encrypt data is minimized since the encryption key doesn't need to be changed when an administrator leaves the job. Encrypting in the device may add cost to that device and the implementation schedule may reflect the natural replacement schedule of storage devices, though this may be offset by the fact that it is being implemented in standard storage devices, and greatly cuts device decommissioning costs and headaches.

Encryption Key Management

Encryption solutions for data-at-rest will be protecting data for potentially very long periods of time. In many ways, the key management system may well be the single most important component of your storage security solution. As we've discussed, you will likely need to maintain keys for many years. You need assurance that the keys used to encrypt data will be available whenever and wherever authorized access to data is required. At the same time, the keys need to be secured so that they themselves aren't compromised (resulting in a data breach). However, key management systems come in many shapes and sizes.

Key Management in the Application

Many applications residing on a run time operating system offer some form of encryption. All encrypting applications must invoke some form of key management. One of the benefits of embedded application key management is that application administrators can also administer key management. From a product development standpoint, embedding key management removes all barriers to release a product by not integrating with a 3rd party key manager.

Unfortunately, there are disadvantages to embedded key management within an application. The obvious limitation is that as more applications offer embedded key management, there are more key managers to manage. Also role separation is difficult since the server or application administrator has root credentials to the application server. Legitimate application users will have access to the application without security admin status. The risk to the keys increases as the number of users increase on the system. Moreover, in any run time operating system, encryption keys are exposed to all vulnerabilities to that operating system. If a vulnerability is discovered, the applications (and your keys) are at the mercy of the operating system vendor's timeline for providing a fix.

From the standards certifications viewpoint, FIPS crypto module certification above level 1 is not possible for application key management since there is no physical security protecting the keys or encryption. The burden of certification must be applied to the entire application which makes it difficult to certify the key management functionality solely. Lastly, the obvious drawback of embedded application key management is that keys are protected with software only. If keys are to be saved for long periods of time, then the protection mechanism of those keys must equal the bit strength of the protected keys.

Key Management in the Device

Many devices today offer embedded encryption and key management. These solutions are very attractive due to their ease of deployment and self-contained nature. They work very well in environments which backup and restore encrypted data using the same device. Key generation and key management are typically external, but integrated encryption (and often compression) is performed within the device itself. Within a device, keys may be protected with hardware security, provided that the device is built with physical protection mechanisms such as an intrusion detector.

Unfortunately, few devices have implemented this level of security. Many devices of this nature receive their keys in cleartext down the storage path or wrap the encryption keys with weaker keys – reducing overall key strength. In addition, many devices that have embedded encryption offer limited key management and almost no centralized key management mechanism. They are able to backup self generated keys, but cannot share them easily. In an enterprise, data-at-rest is considered mobile as backups are created at one location and restored at a distant disaster recovery site. In the absence of centralized key management, key movement becomes a series of repetitive manual administrative tasks to ensure all endpoints have access to encryption keys from all other endpoints.

Stand Alone Key Management Software

Software key management is a valid approach to key management. A standalone key management application is designed to generate, store, and backup key material. One main drawback often seen with key management software is the lack of physical security. This introduces problems with securely storing key material. Additionally, unless an HSM (Hardware Security Module) is used, key material is typically password protected which greatly reduces the bit strength of the actual encryption keys. By reducing the bit strength of the key, you are essentially reducing the amount of time it takes for a hacker to reveal the clear text key, thus enabling the encrypted data to be read. Steps can be taken to secure the server, but redundancy requirements often place key material in many places thus increasing the attack surface.

Centralized Key Management Appliance

Key management as a standalone appliance offers a set of advantages and disadvantages. As a standalone appliance, typically this is more physically secure (assuming the appliance was designed with physical security best practices). Administrators will need to log into the appliance for management and administration, typically with secure multi factor authentication. From an organization security point of view, a self contained key management appliance satisfies compartmentalization requirements.

A centralized key management appliance also offers a potential for transparent key sharing. If all encryption devices are sending their keys centrally, within the capabilities of the appliance, policies could be constructed to allow key movement between encrypting endpoints.

A disadvantage of a key management appliance is that it must employ an API that is widely understood by encrypting devices. Though there are several standards bodies defining a key *management standard, none have emerged as a leader. From an IT administrative point of view, a separate key management appliance must be managed separately. Typically this appliance should be managed by a security specialist. This role is specialized and may be difficult to absorb this skill set within existing IT infrastructure employees.

Vendor Capabilities Matrices

Vendor Encryption

Vendor	Product/Series	Version	Performance	Compression/Decompression
Brocade	Brocade Encryption Switch, FS8-18 Encryption Blade	FOS 6.2	Brocade encryption solutions deliver up to 96 Gbps/sec of disk encryption processing power and with minimum latency	Brocade encryption solutions deliver up to 48 Gbps/sec of compression processing power for tape backup that is provisioned in 24 Gbps blocks
HP	Tape Libraries-ESL/EML/MSL XP 24000/2000 Disk Arrays C-Series MDS 9000 Switches B-Series Encrypting Switches	LTO-4 based libraries Encryption DKA SME (Storage Media Encryption) Encryption SAN Switch	Fast line speed hardware encryption	No impact on compression/decompression of LTO-4 tapes.
IBM	System Storage TS Tape Systems; DS8 series Disk Storage Systems; Tivoli Key Lifecycle Manager	TS 1120/1130 Tape Drives; TS3592 C20 Tape Frame; TS1120 Tape Controller/ TS3100/3200/3310/3500/3494/3400 Tape Libraries; TS3590 Tape Subsystem; TS3953 Library Manager	Scales linearly as storage devices are added, no measurable performance impact	No impact, compression and de-duplication are not affected
NetApp	DataFort Storage Security Appliances	E-Series FC-Series S-Series	FC 1020: 10 Gb/s System Throughput FC 520/525: 2 Gb/s System Throughput S110: 100 MB/s System Throughput E 510/515: 1Gb/s System Throughput	No impact on compression/decompression of tape
Seagate	Self-Encrypting Drives for the Data Center, Desktops and Notebooks	Cheetah, Savvio, Constellation, Momentus	Scales linearly as storage devices are added, no measurable performance impact	Compression and de-duplication capabilities are fully maintained - no impact
Thales	Thales CryptoStor Tape Thales nCIpher netHSM	2.x 2.x	Real-time, wire speed protection of data Network-based, shared encryption for multiple applications	Automatic compression and decompression applied; no impact on de-duplication if performed prior to encryption Fully supports application-based compression

Capabilities Matrix

Data Sharing	Data Replication	Granularity of Encryption	Data Sanitation	Certifi-cation	Vendor
Sharing between internal sites & external partners enabled; data and keys always secured. Sharing of data is controlled by Zoning, LUN mgmt and the configuration of encryption. Zoning and LUN management do not need to be changed to enable encryption.	Encrypted data can be replicated at the LUN, tape or tape pool level. Fully supports data replication, including multi-site recovery.	Encryption of disk drive is established on a per-LUN basis. Encryption of tape is established on a per tape media or tape pool basis.	The products support clearing (overwriting) capabilities according to NIST 800-88.		**Brocade**
Standards based encryption keys (AES-256). Policy-based key sharing groups provide client access control to data.	For tape data replication under control of backup application. Compatible with all data replication capabilities.	Policy-based, per tape cartridge or tape library / partition. XP encryption a per- parity group basis on XP. Switch encryption on a per-tape, or a per-tape volume group basis. For disk: key per LUN. For tape: key per tape, or key per tape pool.	Secure key deletion via Secure Key Manager MSL EK keys cannot be deleted from the token. Token may be physically destroyed. C-Series and XP secure data erasure by deleting encryption key via local key manager	AES-256 encryption	**HP**
2 models, one explicitly has data sharing with no secret key distribution, second has export and import of keys	No impact, data replication efficiencies are maintained	One AES 256 bit key per tape cartridge	Centralized key management makes deletion of key simple and secure	FIPS 140-2 certified	**IBM**
End to end 256 bit key sharing. Ability to create password encrypted key files. Software decryption engine to share data w/3rd parties. Hierarchical Tiered Key Sharing Model. Automated secure key distribution.	Automated Key Sharing with Key Sharing groups.	Global Key Key per Tape Pool Key per Tape Key per LUN (with online rekey support) Key per file share or directory (with online rekey support)	Key deletion with full signed audit log verification.	FIPS 140-2 Level 3 Common Criteria EAL 4+ (FC Series only)	**NetApp**
Data sharing with no secret key distribution	Data replication efficiencies are fully maintained - no impact.	One encryption key per drive, with option for additional keys for separate bands within a drive.	Instant Secure Erase by deleting the encryption key		**Seagate**
Sharing between internal sites and external partners enabled; data and keys always secured Secure key exchange and sharing built-in; option for k of n authentication control	Fully supports data replication, including multi-site recovery Flexible key mgmt allows for easy data replication and recovery	Administrator defined policy down to per tape Per data set with option for k of n multi-administrator authentication to protect data	Key deletion for final data sanitation	FIPS 140-2 Level 3	**Thales**

Vendor Key Management

Vendor	Product/Series	Version	Security of Key Distribution
Brocade	Support for: NetApp Lifetime Key Manager (LKM); HP Secure Key Manager (SKM) EMC/RSA Key Manager (RKM)	LKM - KM500 appliance SKM 1.1 appliance RKM 1.6 appliance	Symmetric key wrapping with secure trustee link. Operating system never processes any key material.
HP	Secure Key Manager (SKM)	1.1	Multi-factor authentication for clients. Keys always distributed over TLS/SSL. TLS security requires FIPS-approved algorithms, when FIPS mode enabled. Configurable IP filtering and key access controls. Configurable admin accounts to limit key access. Backups are encrypted.
	MSL 2024, 4048 & 8096 Encryption Kit (EK)	LTO-4 encrypting tape drive based	Library has separate security login to manage EK. EK requires its own login – cannot use factory default. Keys are only stored in the EK. Transport does not utilize the network.
IBM	Tivoli Key Lifecycle Manager	V1.1	Certificate based cryptographically verified security association, white list of known devices, key material never in the clear outside of keystore and device
NetApp	Lifetime Key Manager	KM500	Symmetric key wrapping with secure trustee link. Operating system never processes any key material.

Capabilities Matrix

Separation of Duties	Re-Key	Lifecycle Mgmt	Certification	Vendor
7 role based administrator login with 2 factor authentication via smart cards.	Re-key function is managed by the selected Key Management System and executed by the encryption device	Automated key lifecycle support. Predefined key expiration and purge time. Ability to mark key as compromised. Hierarchical Key Sharing Groups w/ability to create key silos. Ability to migrate keys between key sharing groups. All key actions tracked with signed audit logs	FIPS 140-2 level-3 in final process March 2009.	**Brocade**
SKM configurable for multiple admin credentials. Configurable admin accounts, allowing any combination of roles/identities. Encrypting clients (tape, switch) do not use admin accounts. Separate admin and security logins for library clients. MSL EK separate admin and security logins for library.	SKM re-keying is automatic, and transparent to the data mover, when data is replicated. MSL EK re-keying is automatic, and transparent to the data mover, when data is replicated.	SKM: All key actions tracked with digitally signed logs, reporting all key lifecycle steps. Policy based key creation and key sharing. Supports key archiving and deletion. Automated, policy-based log management. Tape: key names are associated with the media. MSL EK supports key archiving / backup.	SKM FIPS 140-2 Level 2 validated MSL EK FIPS 140-2 Level 3 hardware.	**HP**
Features of Hardware Security Modules supported permit different types of authentication and roles for access to key material	Re-key without re-encryption supported	Automation of notification of certificate renewal or expiry, automated rollover for use of new groups of keys		**IBM**
7 role based administrator login with 2 factor authentication via smart cards.	Re-key function is managed in KM500 and executed in encryption device	Automated key lifecycle support. Predefined key expiration and purge time. Ability to mark key as compromised. Hierarchical Key Sharing Groups w/ability to create key silos. Ability to migrate keys between key sharing groups. All key actions tracked with signed audit logs	FIPS 140-2 Level 3	**NetApp**

Vendor Solution Descriptions

Brocade

Encryption Solutions
Brocade encryption solutions provide network-based encryption of data from heterogeneous servers to tape libraries and storage subsystems. Brocade products are deployed in the fabric to provide highly scalable solutions delivering up to 96 gigabits per second of disk encryption processing performance. Users deploy Brocade encryption solutions via either the 16 port FS8-18 Encryption Blade for the Brocade DCX Backbones or the 32 port, 2U, rack-mounted Brocade Encryption Switch. These Federal Information Processing Standard (FIPS140-2 Level 3) -compliant encryption solutions can be installed non-disruptively to encrypt plaintext data into encrypted data with unmatched performance. With each port operating at 8 Gigabits/second, Brocade encryption devices offer the highest performance encryption in the industry.

Brocade Encryption Switch and FS8-18 Encryption Blade
Brocade uses NetApp's Lifetime Key Manager, HP Secure Key Manager and RSA Key Manager appliances to manage data encryption keys throughout the life of the encrypted data. Data is encrypted with a 256-bit key according to Advanced Encryption Standard (AES256) algorithms to ensure that data is protected to the highest standards. By teaming with encryption industry experts NetApp, Brocade has created an encryption system that scales to meet the needs of the largest enterprises.

Brocade encryption devices are compatible with NetApp's wide installed base of encryption of data-at-rest devices. With Brocade's large installed base of Fibre Channel storage area networks (SANs), the encryption solutions can be seamlessly incorporated with the largest installed base of storage area networks, including fabrics running Brocade Enterprise OS (EOS) with Brocade M-Series (formerly McDATA) switches.

Brocade encryption solutions are built with the same exacting standards as other Brocade products, as well as published security standards. The Brocade devices use the latest encryption algorithms defined in IEEE 1619 for disk and IEEE 1619.1 for tape. Brocade solutions easily scale up to 96 Gbps of throughput to make encrypting large amounts of data possible.

Brocade understands that organizations must comply with a number of government regulations and offers services to help customers meet the stringent requirements of state and federal mandates. Corporations have entrusted Brocade with their most valuable data for over a decade, and now these same corporations are encrypting their data with Brocade products.

Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
408-333-8000
www.brocade.com
info@brocade.com

Hewlett-Packard

What would happen if your backup tapes or disposed disk drive were lost or stolen? When data at rest is encrypted and encryption keys are secure, the threats of financial loss and damage to your company's reputation are significantly lowered. HP expands data protection to include privacy of the information residing on HP StorageWorks products.

HP StorageWorks Secure Key Manager with ESL/EML LTO-4 Tape Libraries

The HP StorageWorks Secure Key Manager reduces your risk of a costly data breach and reputation damage while improving regulatory compliance with a secure centralized encryption key management solution for HP ESL and EML LTO-4 enterprise tape libraries. The Secure Key Manager automates key generation and management transparent to ISV backup applications. The Secure Key Manager is a hardened server appliance delivering secure identity-based access, administration and logging with strong auditable security designed to meet the rigorous FIPS 140-2 security standards. Additionally, Secure Key Manager provides reliable lifetime key archival with automatic multi-site key replication, high-availability clustering and failover capabilities.

HP StorageWorks XP24000 and XP20000 Disk Array encryption

Customers store their most important mission-critical and confidential data on XP disk arrays therefore HP has introduced a new encryption feature for the XP24000 and XP20000. If a drive is removed from the array, either as a failed drive or through unauthorized access, the data on the drive will be completely meaningless to anyone attempting to read the data. As the data passes through the XP, the final step is for the data to be written to disk by a processor referred to as a DKA. The HP new encryption feature allows the DKA to apply AES 256-bit encryption to the data before it is written to disk. When the data is read back from disk the DKA decrypts the data. There is no measurable performance impact to the array from either the encryption or decryption of the data. Encryption is enabled or disabled on a per-parity group basis. There is a single encryption key per disk array parity group. The encryption key is securely stored in the management station of the array using a key encryption key. The XP's data movement utility, XP AutoLUN, can move data between an unencrypted parity group and an encrypted parity group to facilitate migration of data into a fully secured or encrypted configuration.

HP StorageWorks 1/8 G2 & MSL LTO-4 Encryption Kit

The HP StorageWorks 1/8 G2 & MSL LTO-4 Encryption Kit provides a library-enabled encryption solution that greatly enhances data privacy, confidentiality, and integrity of your critical business data while supporting compliance requirements. While there are a wide range of encryption solutions available, the HP StorageWorks 1/8 G2 & MSL LTO-4 Encryption Kit is intended to be an easy and affordable library-enabled solution for small businesses. One encryption kit is needed per library or autoloader and it must be physically accessible so that the USB token can be inserted into the automation device. One of the two tokens will plug into the USB port in the autoloader or library and will generate and maintain encryption keys for the LTO-4 drives/libraries. The USB key server token uses a hardware random number generator, a cryptographic module running on FIPS 140-2 Level 3 validated hardware, password authentication, and digital envelopes for strong encryption keys and security operations. The second USB token is intended to provide a backup to the first. The keys are transferred securely token-to-token for backup or export, with no exposure to insecure PCs, servers, or networks. The encryption kit provides a self-contained solution for MSL libraries with no additional software, PCs, or servers required or involved.

Encrypting SAN Switches

SANs enable centralized management to support nearly every aspect of the data center. As a result, they are ideal places to consolidate a data-at-rest security strategy with encryption services. HP offers security solutions with both the B-Series and C-Series switches.
- C-Series Fabric Switches with MDS 9000 Storage Media Encryption (SME) using local Cisco key management
- B-Series Encrypting SAN Switches using HP Secure Key Manager

Hewlett-Packard Corporation
www.hp.com/go/encryption

IBM System Storage™

Business data is growing at exponential rates, and along with that growth comes demand for securing the data. Enterprises have responded to that demand by implementing encryption at various layers—in the hardware, on the network and in various applications. This response has resulted in a series of encryption silos—some of it holding confidential customer data—with fragmented approaches to security, keys and coverage.

Different applications across the enterprise often employ different methods of encryption. Some departments in the organization may use public-key cryptography while others use secret-key or hashes. Still others don't encrypt data while it's at rest (such as when it is stored on a device or in a database) but only when the data is in motion, using virtual private networks (VPNs) to secure the data pipeline.

Key management for these encryption approaches is often similarly fragmented. Sometimes key management is carried out by department teams using manual processes or embedded encryption tools. Other times, the key management function is centrally managed and executed. In some cases, there is no formal key management process in place. This fragmented approach to key management can leave the door open for loss or breach of sensitive data.

Deploy a simple solution to a complex problem

IBM Tivoli Key Lifecycle Manager provides a simple solution to the complex problem of key lifecycle management. Traditionally, the more encryption you deploy, the more keys you have to manage. And these keys have their own lifecycles; separate from the data they're protecting—and that lifecycle has to be managed, from initialization and activation through expiration and destruction. Tivoli Key Lifecycle Manager can help you better manage the encryption key lifecycle, allowing you to simplify, centralize, and strengthen your organization's key management processes.

Together with IBM's innovative self-encrypting tape offerings, Tivoli Key Lifecycle Manager offers customers a proven solution that can address their concerns when a tape cartridge or disk drive is removed from the storage system and transported in-house or off-site. Lost storage media is not uncommon these days and brings with it enormous direct and indirect costs for those who lose sensitive information. With IBM System Storage self-encrypting offerings and Tivoli Key Lifecycle Manager, customers no longer have to worry about losing sensitive information should tapes gets misplaced or stolen!

Centrally manage encryption keys

Tivoli Key Lifecycle Manager serves keys at the time of use to allow for centralized storage of key material in a secure location, a unique approach that supports multiple protocols for key serving and manages certificates as well as symmetric and asymmetric keys. Users can also centrally create, import, distribute, backup, archive and manage the lifecycle of those keys and certificates using a customizable graphical user interface (GUI).

Tivoli Key Lifecycle Manager's transparent encryption implementation means that keys are generated and served from a centralized location and are never sent or stored "in the clear." The embedded encryption engine in the IBM self-encrypting tape offerings encrypt and decrypt the data as it enters and leaves the drive at native tape speeds,, which means both faster and more secure handling of data.

Enable strong authentication, strong security

These rich capabilities are made possible by strong authentication between IBM tape storage systems and Tivoli Key Lifecycle Manager. The tape drives are manufactured with a built-in unique certificate. When the drives are mounted, it generates an ephemeral pair of RSA authentication keys. This pair of keys is digitally signed by the tape drive and then sent to the centralized manager, which in turn validates the signature on the generated key pair through the certificate authority. The final step in the process happens when Tivoli Key Lifecycle Manager checks to make sure the device is valid by verifying that it exists in the drive table.

In addition to strong authentication, there is also strong security between the storage device and Tivoli Key Lifecycle Manager. The software generates a session key using the generated key pair from the storage device. Using a pre-generated key, the software then sets an encryption key to be used for an individual cartridge on the storage device. Finally, the software wraps the encryption key with the session key and returns the key to the device.

In addition to protection of the keys and the authentication with the storage device, a list of known devices is maintained so that any unknown device is rejected. With this strategy, a rogue device cannot be deployed on the network and used to intercept organizational data. Nor can the data be intercepted and decrypted as it is being written to or read from the device.

This approach to encryption can dramatically increase data security while simplifying encryption key management. Users don't need to know anything about encryption in order to realize the benefits. Administrators can easily manage a smaller set of more secure keys. And performance isn't impacted because each storage device has hardware built into it that performs at wire speed without latency. Not having to change other processes, install more hardware, or reconfigure software to support it means that the security is kept simple and straightforward.

Leverage flexible implementation options
Tivoli Key Lifecycle Manager can be applied at different levels to simplify key management while meeting the unique needs of your organization.

For organizations that manage keys within separate silos, Tivoli Key Lifecycle Manager can simplify complex key distribution and management, reducing administrative burdens within each silo.

For organizations that want centralized control and policy-driven key management, Tivoli Key Lifecycle Manager offers consolidated management of keys across domains, supports standards that extend management to both IBM and non-IBM products, and integrates well into existing security team methodologies.

For organizations taking a hybrid approach, such as centralized management for storage only, Tivoli Key Lifecycle Manager can make compliance reporting much easier, and can enhance key backup and recovery processes in case of disaster. This approach also enables organizations to establish administrative access based on roles—in this case, storage security.

Simplify key configuration and management tasks
Tivoli Key Lifecycle Manager provides an easy-to-use, Web-based GUI that helps simplify key configuration and management tasks. With this GUI, administrators can easily create keystores, assign keys and certificates, and manage the lifecycle of both from a centralized console.

The software itself is typically installed on your most secure and highly available server or dedicated workstation. Once installed, the GUI allows administrators to perform basic local key lifecycle management on IBM and non-IBM tape drives, and offers not only configuration and setup tools, but also audit and compliance support. The software provides auto-discovery of encryption-capable devices and assigns default keys to each one.

IBM Corporation
www.ibm.com/tivoli

NetApp DataFort Storage Security Appliances

NetApp® has a comprehensive product offering to secure and encrypt data. NetApp offers both a hardware encryption and key management appliances. The DataFort appliance encrypts data at rest in the data path and can be deployed without disrupting the host or storage environment. This allows customers to deploy encryption without costly data migration to encrypting storage arrays.

NetApp E-Series DataFort is a hardened encryption appliance which supports multiple NAS storage protocols. NetApp E-Series DataFort resides in the network between hosts accessing storage and the NAS storage device itself, providing seamless integration to encrypt your data at rest.   NetApp E-Series DataFort offers 2 models to choose from: E510 and E515. Both hardware platforms run the same secure, hardened operating system and offer the same encryption services.

DataFort E-Series Model	E510	E515
Rack Height	2U	1U
Power Supplies	2 hot swappable	1 cold swappable
Fan	2 hot swappable	1 cold swappable
Throughput	1 Gb/s	1 Gb/s
Storage Protocols Supported	CIFS, NFS, DAS, iSCSI	CIFS, NFS, DAS, iSCSI

NetApp E-Series DataFort provides encryption services at the share, export or LUN level. Each share, export or LUN can be assigned a unique 256-bit strength encryption key. E-Series DataFort appliances can be deployed seamlessly by integration into existing storage environments. Real-time re-keying of existing data is available for CIFS and NFS shares.

High availability of encrypted data is ensured by supporting clusters of 2 E-Series DataFort appliances in the event of a failure. Access to encrypted data is maintained through a failover mechanism which automatically detects a failed path and transparently moves services over to the remaining available path.

Secure access to your data at rest is further enhanced through features found in the NetApp E-Series DataFort appliance. Integration with Windows Active Directory ensures automatic import of Windows ACLs. However, the E-Series DataFort also supports an optional DataFort specific ACL as well as pre-approval of group ACL changes to ensure Active Directory Domain Administrators cannot bypass access to encrypted data.

Administration of encrypted shares can be controlled centrally through a DataFort administrator with the appropriate roles, but can also be given to the individual share owners. By allowing individual share owners the ability to manage their encrypted shares, administrative overhead can be significantly reduced and users don't have to wait for a helpdesk ticket in order to manage access to their encrypted share.

NetApp FC-Series DataFort storage security appliances enable complete security for data stored on tape or disk, providing line speed encryption, zero downtime deployment (disk deployments), hardware-based compression (tape deployments) and flexible encryption policies. NetApp FC-Series DataFort offers 3 models to choose from: FC520, FC525 and FC1020. All hardware platforms run the same secure, hardened operating system and offer the same security services.

DataFort FC-Series Model	FC520	FC525	FC1020
Rack Height	2U	1U	2U
Power Supplies	2 hot swappable	1 cold swappable	2 hot swappable
Fan	2 hot swappable	1 cold swappable	2 hot swappable
Throughput	2Gbps	2Gbps	10Gbps
Supported Storage	Disk or Tape	Disk or Tape	Tape

FC-Series DataFort appliances can be deployed transparently through their ability to perform in-place encryption of existing data. This means zero downtime for applications that require encryption services. Each block of data is encrypted as a background process until all designated LUNs are 100% encrypted.
Hardware based compression means that encryption will not increase media usage. By performing compression prior to encrypting the data, the FC-Series DataFort appliance ensures offsite tape security without increasing operational costs.

FC-Series DataFort appliances can be deployed with numerous types of encryption policies. Each disk LUN can be assigned a unique 256-bit strength encryption key which can be periodically rotated to comply with company policies or regulations as needed. For tape deployments, individual encryption keys can be assigned to a backup application pool or even down to the individual media ID level for complete cryptographic compartmentalization. Individual keys for each backup tape means loss of an individual tape does not put any other encrypted media at risk.

Some of the common applications for FC-Series DataFort include

- Compartmentalize data in shared storage
- Secure backup and disaster recovery locations
- Secure tape media for transit and off-site storage
- Secure SAN disks for disk repair or disposal
- Enable regulatory compliance
- Secure outsourcing and off shoring

NetApp S-Series DataFort appliances offer a solution to extend encryption services to data stored on SCSI tape drives. As large enterprises deploy encryption across their infrastructure, many are realizing a need for heterogeneous storage support. SCSI tape drives encompass a significant portion of many enterprises infrastructures. S-Series DataFort appliances offers protection of these investments by allowing these drives to participate in the same encryption features offered by the NetApp DataFort product line.

NetApp DataFort S-Series	S110
Rack Height	2U
Power Supplies	2 hot swappable
Fan	2 hot swappable
SCSI Connection	VHDCI LVD-SCSI
Bus Speed	U160

Security and Usability Features Common to NetApp Storage Security Products
All NetApp Security Appliances support creation of administrators with granular, customizable roles. Each admin role is only allowed a subset of duties, allowing distribution of responsibilities amongst multiple individuals. Both NetApp DataFort and Lifetime Key Management Appliance are flexible enough to allow creation of custom administrator roles by combining multiple roles into an administrator which suits each company's unique needs. The table below is an example of 2 roles and lists a few of their functions:

Administrator Role	Function
Key Administrator	Generation of encryption keys, control of key import and export
Account Administrator	Add/Delete administrator accounts, assign/revoke smart card requirements for authentication

In order to provide an irrefutable audit trail for encrypted data access and administrator activity, secure audit logging is available for all NetApp Storage Security appliances. Each log message can be cryptographically signed and can only be verified on the appliance which originated the message. Attempts to modify the signature or the logs themselves can be easily verified for integrity and authenticity.

Lastly, DMC is a software management console that provides a centralized view of all NetApp security products such as DataFort and the KM500. From a single viewpoint, an Administrator can configure DataFort appliances and configure key sharing policies on the KM500. The administrator can also view system interconnect topologies and drill down to view individual appliance status and alerts.

http://www.netapp.com

NetApp KM500 Lifetime Key Management Appliance

NetApp® has a comprehensive product offering to secure and encrypt data. NetApp offers both a hardware encryption and key management appliances. The NetApp Lifetime Key Management™ Appliance enables global key management and data policy enforcement. The entire NetApp security system can be managed centrally via DMC, a global management software user interface.

The NetApp KM500 Lifetime Key Manager is NetApp's 4th generation key management product. The KM500 is a hardened, tamper proof, appliance that provides secure key archive and distribution of encryption keys. The KM500 offers a rich key management feature set that is a direct result of supporting complex and geographically dispersed NetApp security customers. The KM500 supports dynamic systems generating many keys in many locations while efficiently and securely enforcing key sharing policies.

The NetApp KM500 offers the following security features and certifications:
- Validated to FIPS 140-2 Level 3
- Prevents theft of appliance via removable system ignition card
- Recovery cards enforce split trust model for appliance recovery and sensitive actions
- Appliance intrusion detection circuitry
- Cryptographic Security Encryption Processor to process all cryptographic functions
- 7 unique role based administrator functions
- Hierarchical key sharing support
- OpenKey API to support partner encrypting products
- High entropy key generation protects against predicting future keys
- End-to-end 256-bit strength security for key movement

The NetApp KM500 appliance can be linked to other KM500 appliances to provide high availability of encryption keys. Up to 16 KM500 appliances can be linked together to support up to 1000 DataFort appliances.

NetApp Lifetime Key Management Appliance	KM500
Rack Height	2U
Power Supplies	2 hot swappable
Fan	2 hot swappable
Hard Drives	2 hot swappable drives - RAID 1
Key Capacity	10 million

NetApp's Lifetime Key Management Appliance supports the following encrypting devices: Optica Eclipz Product Line, Brocade Encrypting Fabric Product Line and NetApp DataFort Product Line. Partner support enabled via OpenKey API, a simple key management API for partner encrypting products.

http://www.netapp.com

NetApp™

Seagate Encryption Solutions Self-Encrypting Drives

IT departments retire drives daily in order to:
- Return for Warranty, Repair, Expired Lease
- Repurpose or retire the drive

The costs to retired these drives securely by overwriting the drive's data or destroying the drive are high. Self-Encrypting Drives reduce the cost of retiring drives, and preserve the value of the retired drive by enabling the drive to be securely repurposed or returned for service, warranty or expired lease. Self-Encrypting Drives are secure the moment the drive is unplugged. They free IT from drive control headaches and disposal costs. They provide compliance "safe harbor" without hindering IT.

IBM, LSI, and Dell are building Self-Encrypting Drives into solutions. Self-Encrypting Drives deliver these benefits:

Robust Security
- The United States NSA qualified Self-Encrypting Drive for National Security Systems. Qualification has been received for the first self-encrypting drive model.
- No clear text secrets anywhere on the drive. Not susceptible to cold-boot attack.
- No exposure of encrypted text (encrypted text is an aid to an attacker)

Performs at full drive speed
- Dedicated engine for full interface speed encryption
- Scales linearly, automatically
- Granular data classification not needed. All data can be encrypted, with no performance hit

Management made simple

    Instant secure erase mode doesn't require key management during normal operation. The owner simply deletes the encryption key in the drive when ready to retire or repurpose the drive.

    Auto-locking mode uses simplified key management to secure the drive from misplacement, loss during normal operation:
- Integrated - encrypts data-at-rest with an embedded encryption key and password authentication
- Transparent to OS, applications, application developers, databases, database administrators
- Data compression and de-duplication efficiencies are fully maintained in the storage system.
- Encryption keys don't leave the drive. No need to track or manage them. No data re-encryption needed when re-keying exposed keys. Access control credentials are separate from the encryption key.
- Standards-based; Interoperable: The world's top six hard drive vendors collaborated to develop the final enterprise specification published by the Trusted Computing Group (TCG). This specification, created to be the standard for developing and managing Self-Encrypting Drives, enables SEDs from different vendors to be interoperable.

Seagate Technology
1-800-SEAGATE
www.Seagate.com and www.FDESecurityLeaders.com

Thales CryptoStor Tape

Tape media is the most common means of archiving enterprise data. All too often, removable media is lost, stolen, or compromised. When that happens, unauthorized users can read tape data, analyze confidential information, and even rebuild entire systems without a trace. The resulting damage— both direct and to reputation—can be massive. Encryption provides the only failsafe security mechanism for archived data, but many organizations fear it will require costly infrastructure changes, lengthen backups, or make data difficult or impossible to retrieve.

Encryption without disruption
An in-line, high-speed tape encryption appliance, Thales CryptoStor Tape delivers enterprise-class data protection and privacy for tape media. It encrypts tape data and provides automated key management with minimal impact to operations. Native tape drive performance remains unchanged.

Integrates with existing processes
Thales CryptoStor Tape works with your existing backup applications, receiving data from servers and passing encrypted data to tape libraries. It can operate alone or be clustered. Multiple appliances can be distributed to different locations, as needed.

Thales nCipher netHSM

Organizations have more information worth protecting than ever before. Confidential customer data, financial results, and research findings are just a few types of sensitive information at risk. Even the encryption keys that are critical to protecting this data can be vulnerable to attack. Ineffective protection of these keys can lead to financial fraud, loss of intellectual property, and brand damage.

Software protection falls short
Companies face both logical attacks over their networks and physical breaches by staff or intruders. Hackers can use malicious code to capture critical data and the underlying encryption keys. Thieves can quickly copy sensitive data or install backdoors. As these threats evolve, software-based security cannot keep up. Recent research has reaffirmed the weaknesses of even the most advanced software security measures.

Safeguard data and processes within hardware
nCipher netHSM provides encryption processing, secure code execution, and key protection inside a highly secure, tamper-resistant hardware environment. Critical information is never exposed, so it's much less vulnerable to compromise, whether threats originate within or outside the organization.

Scalable and cost-effective hardware for strategic security initiatives
nCipher netHSM is a shared security module that processes and protects encryption keys, critical executable code, and highly confidential data for several network resources. With nCipher netHSM, sensitive information is safe from logical and physical attacks, enabling you to confidently manage identities, passwords, and critical processes.

Thales Corporation Ltd.
Europe, Middle East, Africa
THALES e-SECURITY LTD. Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ. UK
T: +44 (0)1844 201800 F: +44 (0)1844 208550 E: emea.sales@thales-esecurity.com

Americas
THALES e-SECURITY, INC. 2200 North Commerce Parkway, Suite 200, Weston, Florida 33326. USA
T: +1 888 744 4976 or +1 954 888 6200 F: +1 954 888 6211 E: sales@thalesesec.com
Asia Pacific
THALES TRANSPORT & SECURITY (HONG KONG) LTD. Units 2205-06, 22/F Vicwood Plaza, 199 Des Voeux Road Central, Hong Kong, PRC
T: +852 2815 8633 F: +852 2815 8141 E: asia.sales@thales-esecurity.com

THALES

Wave Systems Corporation Embassy Trust Suite for Self Encrypting Drives

Industry leading hardware security management solutions, including key management, for managing industry standard trusted computing hardware components in personal computers. The following hardware components are supported:

- Self Encrypting Drives from Seagate, Samsung, Fujitsu, Toshiba, and Samsung
- Trusted Platform Modules
- Biometric Finger Print Readers
- Smart Card Readers, both contact and contactless.

These components are enabled to support the following applications:
- Secure Authentication
- Data Protection
- Network Access Control

Embassy Security Center / Embassy Trusted Drive Manager

- Management of client security hardware including Trusted Platform Modules (TPM) and Full Disk Encrypting (FDE) hard drives.
    - Complete life cycle management including initialization/provisioning, password management, control and recovery, user management, pre-boot authentication setup, and recommissioning/ decommissioning of TPMs and FDE drives.
- Strong authentication including biometrics, smart cards, and TPM-secured digital certificates
    - Pre-Boot authentication for FDE drive unlocking with Single Signon and Windows password synchronization
- Compliance enabled for centralized management, audit logging, and user key recovery
- Robust multivendor and multiplatform support for data protection hardware
- Support for the new Trusted Computing Group Opal Storage Subsystem Class specifications.
- Microsoft Windows XP and Vista

Embassy Remote Administration Server

- Complete remote management of Trusted Platform Modules and Full Disk Encrypting drives with enterprise security policy enforcement
- Facilitates easy deployment and enterprise management of trusted platforms
- Automatic user key management including backup and recovery of lost passwords
- Integration with Microsoft management infrastructure including Active Directory, and General Policy Objects
- Generates secure device activity logs for data protection compliance reporting and auditing
- Microsoft Windows Server 2003/2008, Windows XP w/MMC snap-in

Wave Systems Corp.
480 Pleasant Street
Lee, MA 01238
(877) 228 – WAVE
www.wave.com

About the SNIA Storage Security Industry Forum

The SNIA Storage Security Industry Forum (SSIF) is a consortium of storage professionals, security professionals, security practitioners, and academics – all dedicated to fulfill the Storage Networking Industry Association (SNIA) vision to increase the overall knowledge and availability of robust security solutions in today's storage ecosystems.

The SSIF delivers on the SNIA security vision by consolidating our vast body of knowledge and practical experiences in security and storage into high quality educational, technical, and engineering activities that influence the design, use, and management of storage technology to better protect and secure information. We're actively identifying best practices on building secure storage networks, providing education on storage security topics, and participating in standards development. Our goal is to provide data and information security expertise to contribute to a better understanding of information assurance and how it applies in the organization. For more information, please visit the SSIF website at **www.snia.org/ssif**.